

Module 1: Networking Today

1.0 Introduction

1.0.1 Why should I take this module?

Welcome to Networking Today!

Congratulations! This module starts you on your path to a successful career in Information Technology by giving you a foundational understanding of the creation, operation, and maintenance of networks. As a bonus, you get to dive into networking simulations using Packet Tracer. We promise you will really enjoy it!

1.0.2 What will I learn to do in this module?

Module Title: Networking Today

Module Objective: Explain the advances in modern network technologies.

Topic Title	Topic Objective
Networks Affect our Lives	Explain how networks affect our daily lives.
Network Components are used.	Explain how host and network devices are used.
Network Representations and Topologies how they are used in network topologies	Explain representations and used in network topologies
Common Types of Networks common types of	Compare the characteristics of networks
Internet Connections interconnect to the	Explain how LANs and WANs interconnect to the internet
Reliable Networks reliable	Describe the four basic requirements of a network.
Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.

Network Security all	Identify some basic security threats and solution for networks.
-------------------------	--

The IT Professional networking field.	Explain employment opportunities in the
--	---

1.0.3 Download and Install Packet Tracer

To obtain and install your copy of Cisco Packet Tracer, please follow the instructions from the link below:

<https://www.netacad.com/resources/lab-downloads>

1.0.4 Video - Getting Started in Cisco Packet Tracer

Packet Tracer is a tool that allows you to simulate real networks. It provides three main menus:

You can add devices and connect them via cables or wireless.

You can select, delete, inspect, label, and group components within your network.

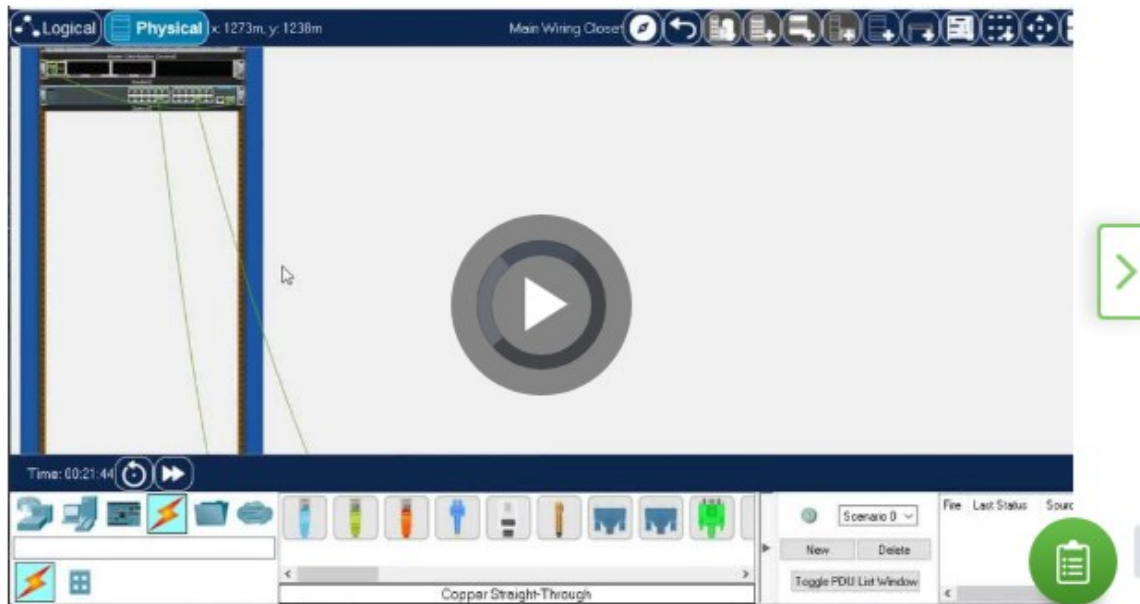
You can manage your network by opening an existing/sample network, saving your current network, and modifying your user profile or preferences.

If you have used any program such as a word processor or spreadsheet, you are already familiar with the File menu commands located in the top menu bar. The Open, Save, Save As, and Exit commands work as they would for any program, but there are two commands that are special to Packet Tracer.

The Open Samples command will display a directory of prebuilt examples of features and configurations of various network and Internet of Things devices included within Packet Tracer.

The Exit and Logout command will remove the registration information for this copy of Packet Tracer and require the next user of this copy of Packet Tracer to do the login procedure again.

Click Play in the video to learn how to use the menus and how to create your first Packet Tracer network.



Transcript

Follow along using the transcript.

00:00

- [Instructor] Hello everyone.

00:01

Welcome to our Getting Started in Cisco Packet Tracer

00:04

Walkthrough video.

00:06

In this video, I get to show you the different features

00:09

built inside of the program known as Cisco Packet Tracer.

00:12

As we get started, we'll highlight some of

00:14

the key components of using

00:16

the Cisco Packet Tracer application.

00:19

Let's begin by taking a look at the bottom toolbar

00:21

and I'm looking at the bottom left corner.

00:24

Here, we have a variety of different categories

00:26

and in each category we're going to have options below.

00:29

For example, the default category is Network Devices.

00:32

That's selected by default.

00:34

In the Network Device category, we'll find the sub category

00:37

of Routers.

00:38

With Routers selected, we'll see a variety of different

00:41

model routers available for us to put into our topology.

00:46

If I click on the next item it's Switches

00:49

inside of our Network Device category.

00:51

And then my list will now contain network switches

00:55

that I can deploy inside of my topology above.

00:58

The next category is Hubs followed of course

01:01

by Wireless Devices, including then the next category

01:06

of Security

01:08

and then finally is WAN Emulation

01:11

for our wide area networks.

01:14

Outside of the Network Device category, we can find the next

01:17

main category of End Devices.

01:20

If I click on End Devices, our default subcategory

01:23

is in end devices of different types of hosts

01:27

and other equipment we can put on our network.

01:31

There's another sub category for End Devices, which is Home.

01:35

And this brings in a lot of our smart network enabled

01:38

IOT devices.

01:41

We can go further by looking at citywide devices, which are

01:44

under the category of Smart City within End Devices.

01:49

If we continue on the next component will be Industrial

01:53

and then even Power Grid.

01:56

All bringing some great features into Cisco Packet Tracer

01:59

and the type of devices we can deploy in a network.

02:03

To go even a further into the realm of internet of things

02:05

known as IOT, we have another main category known as

02:09

Components and in Components you'll find a variety

02:13

of different boards.

02:14

Also, we have another subcategory for Actuators

02:18

and even Sensors.

02:20

These can be deployed in a network just like

02:23

what we're doing now.

02:25

To interconnect your devices, we'll be utilizing

02:28

the Connections category.

02:31

In the Connections category, we have two sub categories.

02:34

We have Connections, which is a common type of cabling

02:37

we'll be using but also another sub category

02:40

is Structured Cabling.

02:42

And here you will find items that are available

02:44

in Physical View of Cisco Packet Tracer.

02:47

And these will include patch panel connectors

02:49

and wall mounts.

02:51

The next category is Miscellaneous and here we will find

02:54

some custom made devices with components already installed.

03:00

Lastly, the category of Multiuser Connection

03:03

allows us to interconnect our Packet Tracer instance

03:06

with others across our local area network

03:08

or even a wide area network connection.

03:12

Let's continue by creating a small network

03:15

utilizing our Cisco Packet Tracer Logical View.

03:20

By default, we can see our Packet Tracer here has opened

03:22

in the logical view mode.

03:24

This is where we can build a logical topology.

03:27

I'm going to select the main category

03:29

in the bottom toolbar of Network Devices.

03:32

The default selection again is Routers.

03:34

And I'll go ahead and take a look at the routers available.

03:38

At this time, I may want something like

03:41

a 4331 Cisco router.

03:44

I can click on that and then I can click in

03:46

our logical topology.

03:48

I can continue by deploying now a network switch.

03:52

I will click on the sub category for Switches

03:55

then I'll click the first switch available.

03:58

I will then click on my logical topology

04:01

and now it is ready.

04:04

At this time, I'd like to add on two or three end devices.

04:08

So I'll click on the category of End Devices.

04:12

The default sub category of our End Devices

04:15

is already selected.

04:17

And I will go ahead and take one PC and click it on,

04:20

put it right into the logical topology and one laptop.

04:24

I will click and then click on the logical topology.

04:28

At this time, I'd like to interconnect these by utilizing

04:31

our cabling.

04:32

That is under our Connections category.

04:37

I will click on Connections.

04:38

The default sub category of Connections is already selected

04:42

and I will choose the appropriate cabling to interconnect

04:46

these devices with a router and switch.

04:50

I will use my straight-through cable

04:52

which is the third option available.

04:54

I will select it, click on my PC,

04:57

choose the corresponding port of Fast Ethernet

05:01

and connect that to the switch.

05:04

I'm going to choose any available interface

05:06

for network connectivity.

05:09

I will repeat this by connecting the cable from the laptop

05:14

Fast Ethernet

05:17

to the switch on another available network interface.

05:22

Lastly, I'll interconnect that switch to the router

05:25

in our logical topology.

05:27

I will grab the appropriate cable by clicking on it,

05:30

click on an available port on the switch

05:34

and then connect it to the router

05:36

on available network connection.

05:41

You will see indicator lights being shown here

05:43

due to a port status and connectivity.

05:47

At this time, we have a small logical topology built.

05:51

We will take a look at the physical topology

05:54

of how we will be able to build a network

05:56

and interconnect them in the Physical View.

06:00

I will click on the Physical tab and you'll see a change.

06:05

The change is our screen is a little bit taller.

06:08

The bottom toolbar might be in the way.

06:11

We will have our ability to scroll on the right side

06:14

of our screen by the sliding tab.

06:17

We can see that there's the PC that I have clicked

06:21

and put in the logical topology along with a cable

06:23

coming off of it.

06:25

Also, we can see the laptop has been positioned

06:28

on top of the PC.

06:29

I can click and drag it and put it on the table

06:32

next to the PC.

06:35

If I scroll up, you'll see those cables

06:37

from the PC and the laptop connecting to the switch.

06:40

I can click and drag the switch and I can lower it

06:44

on our network rack.

06:46

That switch is connected to the router.

06:49

I can click and lower the router on the network rack

06:52

in order to organize these devices and cabling better.

06:57

In the Physical View, I have the ability to use

06:59

my main toolbar and I have settings for zoom.

07:03

I will click the magnifier glass with a plus to zoom in.

07:09

Now you have a better view of the physical router

07:13

with the cable that connects to the physical switch.

07:16

And then if I scroll down the physical switch

07:19

with the two connections to the devices down below.

07:25

If we want to manage our cabling, we'll right click

07:28

on a network cable and we'll be presented

07:30

with three options.

07:31

We can delete the cable to remove it completely.

07:34

We can color the cable a different color so we can identify

07:38

the cable and thus identify any devices connected

07:41

by that cable easier.

07:43

Or we can select Manage Cable, which will take the cable

07:46

and will put it away nicely, which provides us a nice

07:49

and tidy workspace.

07:50

In the real physical world that would allow us to organize

07:53

our cabling, secure them appropriately

07:56

and keep them from disconnecting or from being crimped.

07:59

We cannot use Manage Cable at this time for any devices

08:03

sitting on a table or on a shelf.

08:06

We can only use this Manage Cable option when devices are

08:10

on our network rack on the left side.

08:13

At this time, I'll scroll up to the top and you can see

08:16

that we have our switch and our router.

08:19

I can right click on the switch

08:20

and I can say Manage All Cables on Device.

08:24

When I select that, you will see that the cabling

08:27

between the switch and the router looks like it disappears.

08:30

Instead of it just keeping our cables nice and tidy

08:33

between the actual switch connection

08:35

to the upstream router connection.

08:38

If I right click on that switch again, you'll see

08:40

we have the options to Inspect Front, Inspect Rear

08:44

to Delete the Device or to Unmanage All Cables

08:47

on the Device as well.

08:48

By unmanaging all cables on the device, we see

08:51

the interconnected cable between the router and the switch

08:54

reappear, hanging down on the front of our network rack.

08:58

If I right click on that switch and select Inspect Front

09:01

we'll get a closer view of our network switch.

09:05

Again, we have our magnifier glass options to zoom in.

09:08

I will click on zoom in and then I will scroll to the right

09:12

and down with my Packet Tracer window.

09:15

We can see that I have port 10 on the switch connected

09:18

to a device.

09:19

If I hover over that connection, we'll see it's connected

09:22

to device PC zero.

09:25

We'll also see there's a link light on for port 20.

09:28

If I hover over that connection, we'll see that this

09:31

connection goes down to the laptop.

09:33

And lastly, if I hover over the gigabit connection

09:37

on the far right side of the switch

09:38

we'll see that this connects to device router zero.

09:42

This is great information for us to be able to document

09:44

and visualize our interconnected physical network.

09:48

But also if I close this off

09:51

again, we can just follow those cables

09:53

and see where the interconnect to the devices.

09:56

If I right click on the switch,

09:57

we can also select Inspect Rear.

10:00

When we click Inspect Rear,

10:02

we will get a rear view of the Cisco switch.

10:06

Again, I'll use my magnifier glass and we will be able

10:09

to click and zoom in.

10:11

Here we will see the console connection for us to complete

10:14

our initial configuration of the switch.

10:17

Also, you'll notice that there's no power button

10:19

on the Cisco switch because the Cisco switch is

10:21

automatically powered on once it is connected

10:23

with a power cable.

10:25

To remove power, we would unplug the Cisco switch

10:28

from any power source.

10:31

If I scroll back to the left side

10:33

we can do the same with router zero.

10:34

We can right click and Inspect Front

10:37

and we can zoom in and get a better view

10:39

of the Cisco router and any connections as well as

10:43

any available slots that we can install any

10:46

new components or additional features on.

10:52

I can right click on the router again

10:53

and click on Inspect Rear.

10:55

And again, I'll zoom in and here on the router

10:58

we can see that we have an aux port.

11:01

We have our console port as well as we have

11:04

a management interface.

11:06

On the right side, we'll see that we have a power button

11:09

and the current status of the router is powered on.

11:12

If I click the power button, the green light will turn off

11:14

and the power is now disabled for the router.

11:18

I click it on again and now the router is actually

11:20

booting up since it has received power.

11:24

I will click the X to close the rear view

11:27

of the Cisco router.

11:30

If we want to deploy new devices onto this current

11:33

physical topology, we will use our bottom toolbar.

11:37

I will select End Devices and in the End Device subcategory

11:41

I would like to deploy a server.

11:43

I can click on the server and I will click on

11:47

the network rack.

11:49

That server is now deployed on the network rack.

11:52

We can see that it is powered on and that we have

11:55

a network interface ready for connection.

11:58

I will go ahead and click on Connections

12:00

and I will click on a straight through cable.

12:03

When I click on this straight through cable

12:05

I will click on the network interface card

12:07

for Fast Ethernet zero of the server.

12:10

And then I will click on any port I would like

12:12

to connect it to.

12:13

If you want a closer view of what port I'm connecting it to,

12:16

I can always right click on the switch

12:18

and click Inspect Front and zoom in for a closer view.

12:24

With the zoomed in front of the switch

12:26

I can easily identify what port of the switch

12:29

I would like to connect to.

12:31

For example, I would like to connect to port 24

12:34

which is FE 0/24 on this 2960 switch.

12:39

When I click on that port, the cable is now connected.

12:42

If you feel that the cable is getting lost you can always

12:45

right click on that cable and change the color

12:48

as we mentioned earlier

12:50

I can make it red for example, and click Okay.

12:53

And now it's much easier to find the connection

12:55

from the server to that Cisco switch.

12:58

This is the power of Cisco Packet Tracer utilizing

13:00

the Logical and the Physical Views.

13:04

Please practice and enjoy using Cisco Packet Tracer

13:07

for all of your network configurations

13:09

and for any scenarios that

13:10

you could possibly imagine and build.

1.0.5 Packet Tracer - Logical and Physical Mode Exploration

The network model in this Packet Tracer Physical Mode (PTPM) activity incorporates many of the technologies that you can master in Cisco Networking Academy courses. It represents a simplified version of how a small to medium-sized business network might look.

Most of the devices in the Seward branch office and Warrenton data center are already deployed and configured. You have just been hired to review the devices and networks deployed. It is not important that you understand everything you see and do in this activity. Feel free to explore the network on your own. If you wish to proceed more systematically, follow the steps below. Answer the questions to the best of your ability.

Logical and Physical Mode Exploration
Exploration

Logical and Physical Mode

1.1 Networks Affect our Lives

1.1.1 Networks Connect Us

Among all of the essentials for human existence, the need to interact with others ranks just below our need to sustain life. Communication is almost as important to us as our reliance on air, water, food, and shelter.

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents.

1.1.2 Video - The Cisco Networking Academy Learning Experience

World changers aren't born. They are made. Since 1997 Cisco Networking Academy has been working towards a single goal: the educating and skill building of the next generation of talent required for the digital economy.

Click Play to how Cisco Networking Academy to learn how we use technology to make the world a better place.

Actual video

Transcript

Follow along using the transcript.

Show

Transcript

Transcript

16px (

default

)

English

00:00

- [Narrator] This is the world always moving,

00:03

always changing, and nowhere is that more true

00:06

than in technology.

00:09

From the very start we've been on a quest

00:11

to make things easier, move faster,

00:14

and expand our opportunities.

00:16

And with each new innovation,

00:18

the pace of change has only accelerated.

00:21

To keep up, education has to advance and evolve as well.

00:26

At Cisco Networking Academy we believe

00:29

that powerful learning comes from hands-on instruction

00:31

with real equipment and software,

00:33

so we're committed to giving our students

00:35

a real-world grounding in today's most valuable skills.

00:39

We've developed many of our own tools

00:41

including simulators that help them test

00:43

their ideas at scale in different environments,

00:45

and we keep it real by giving students the chance

00:48

to test their skills in competitions and hackathons.

00:51

They receive personalized feedback every step of the way

00:54

and not just from instructors,

00:56

automated performance-based feedback is

00:58

an integral part of the learning experience.

01:01

Our classes are translated in up to 20 languages

01:04

making it easier to learn in your own language

01:06

and share experiences with others around the world.

01:09

More than technical skills,

01:11

it's a broad-based program focused on creating

01:13

global problem solvers ready to move the world forward.

01:18

Our students become t-shaped professionals,

01:21

meaning they get deep technical knowledge

01:23

and at least one or two high demand job areas.

01:27

But they also get the broader range of skills needed

01:29

to collaborate across related technologies,

01:32

which makes them even more valuable to potential employers.

01:36

Preparing students to become the innovators

01:38

of tomorrow capable of successfully contributing

01:41

to multidisciplinary teams that are setting the pace

01:44

for the future of networking,

01:46

the Internet of Things, security, programming,

01:49

and information technology.

01:51

They learn from the best trained instructors

01:53

and earn certifications that can get them better jobs,

01:56

higher pay and a well-rounded career

01:59

meeting today's needs and tomorrow's opportunities.

02:03

There's no saying where technology will take us next.

02:06

Only that the ones leading away

02:08

will have the t-shaped skills you get

02:10

at Cisco Networking Academy.

02:12

It's how Academy's, educators, and students keep ahead

02:15

of an ever-evolving world.

02:17

Discover the latest courses

02:18

and set out on an exciting career journey at netacad.com.

02:22

(soft music)

1.1.3 No Boundaries

Advancements in networking technologies are perhaps the most significant changes in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant, presenting ever-diminishing obstacles.

The internet has changed the manner in which our social, commercial, political, and personal interactions occur. The immediate nature of communications over the internet encourages the creation of global communities. Global communities allow for social interaction that is independent of location or time zone.

The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe.

The creation of the cloud lets us store documents and pictures and access them anywhere, anytime. So whether we are on a train, in a park, or standing on top of a mountain, we can seamlessly access our data and applications on any device.

1.2 Network Components

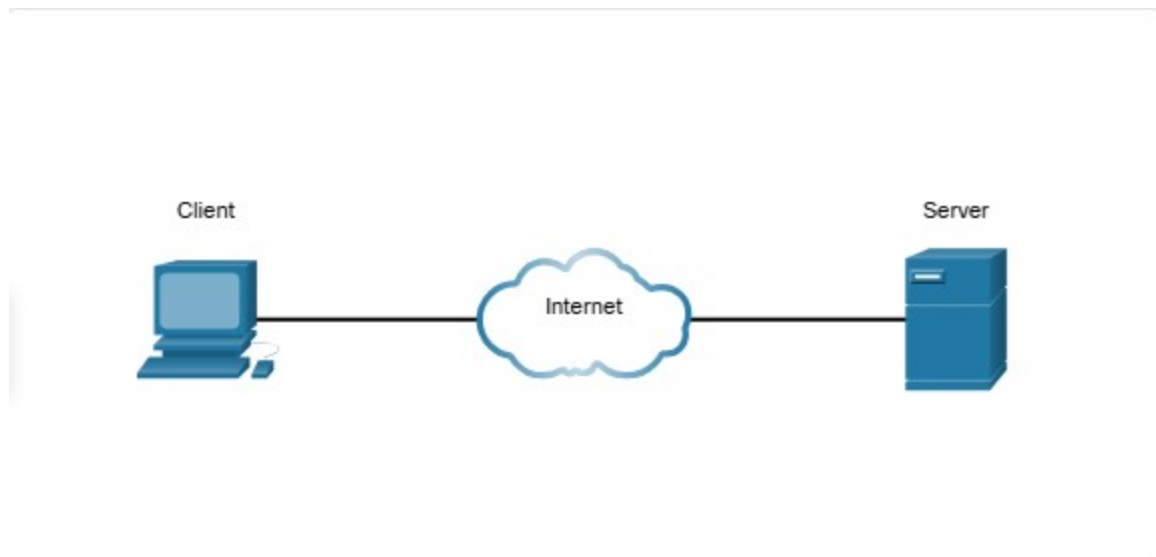
1.2.1 Host Roles

If you want to be a part of a global online community, your computer, tablet, or smart phone must first be connected to a network. That network must be connected to the internet. This topic discusses the parts of a network. See if you recognize these components in your own home or school network!

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end devices. Some hosts are also called clients. However, the term hosts specifically refers to devices on the network that are assigned a number for communication purposes. This number identifies the host within a particular network. This number is called the Internet Protocol (IP) address. An IP address identifies the host and the network to which the host is attached.

Servers are computers with software that allow them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software. For example, a server requires web server software in order to provide web services to the network. A computer with server software can provide services simultaneously to many different clients.

As mentioned before, clients are a type of host. Clients have software for requesting and displaying the information obtained from the server, as shown in the figure.



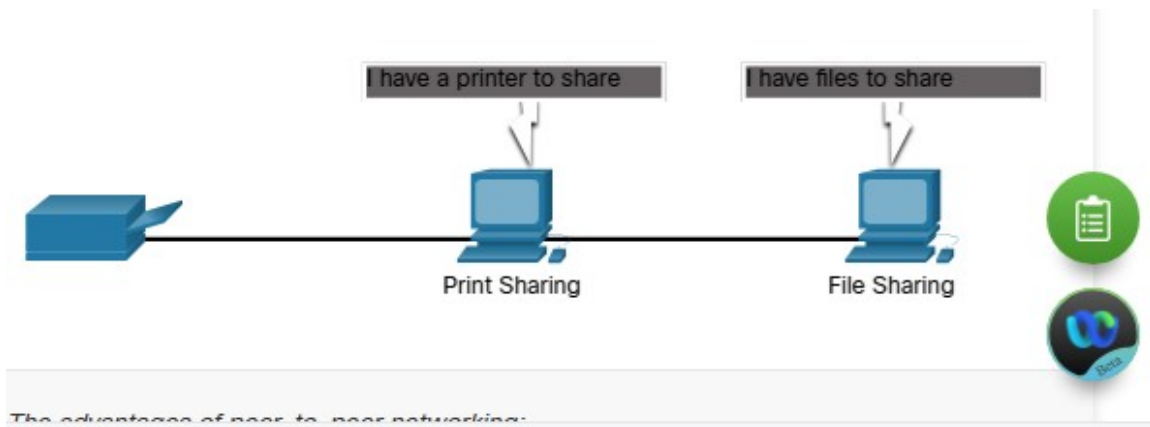
An example of client software is a web browser, like Chrome or FireFox. A single computer can also run multiple types of client software. For example, a user can check email and view a web page while instant messaging and listening to an audio stream. The table lists three common types of server software.

Type	Description
Email	The email server runs email server software. Clients use email client software, such as Microsoft Outlook, to access email on the server.
Web	The web server runs web server software. Clients use browser software, such as Internet Explorer, to access web pages on the server.
File	The file server stores corporate and user files in a central location. The client devices access these files with client software such as Windows File Explorer.

1.2.2 Peer-to-Peer

Client and server software usually run on separate computers, but it is also possible for one computer to be used for both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network.

In the figure, the print sharing PC has a Universal Serial Bus (USB) connection to the printer and a network connection, using a network interface card (NIC), to the file sharing PC.



The advantages of peer-to-peer networking:

Easy to set up

Less complex

Lower cost because network devices and dedicated servers may not be required

Can be used for simple tasks such as transferring files and sharing printers

The disadvantages of peer-to-peer networking:

No centralized administration

Not as secure

Not scalable

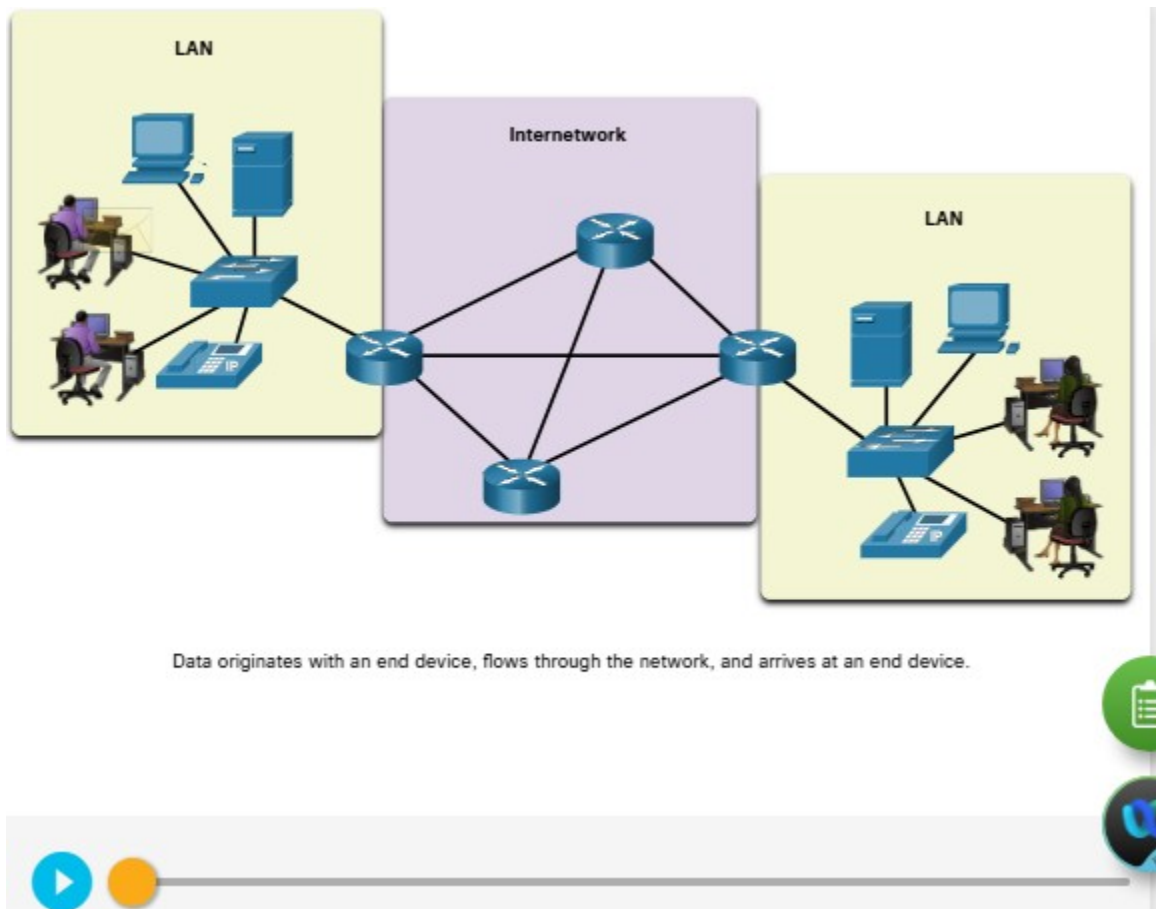
All devices may act as both clients and servers which can slow their performance

1.2.3 End Devices

The network devices that people are most familiar with are end devices. To distinguish one end device from another, each end device on a network has an address. When an end device initiates communication, it uses the address of the destination end device to specify where to deliver the message.

An end device is either the source or destination of a message transmitted over the network.

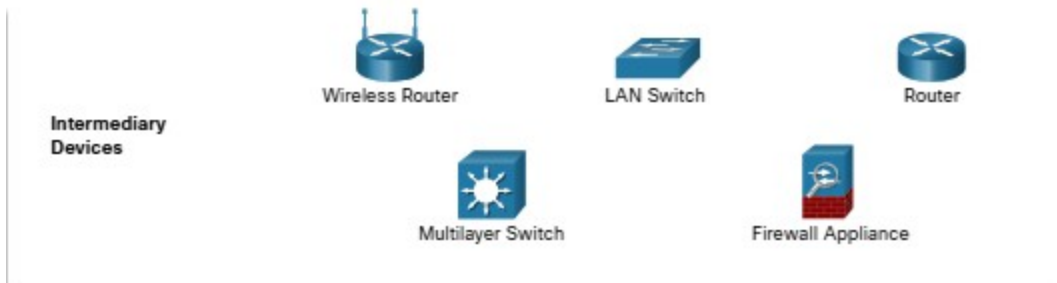
Click Play in the figure to see an animation of data flowing through a network.



1.2.4 Intermediary Devices

Intermediary devices connect the individual end devices to the network. They can connect multiple individual networks to form an internetwork. These intermediary devices provide connectivity and ensure that data flows across the network.

Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. Examples of the more common intermediary devices and a list of functions are shown in the figure.



Intermediary network devices perform some or all of these functions:

Regenerate and retransmit communication signals

Maintain information about what pathways exist through the network and internetwork

Notify other devices of errors and communication failures

Direct data along alternate pathways when there is a link failure

Classify and direct messages according to priorities

Permit or deny the flow of data, based on security settings

Note: Not shown is a legacy Ethernet hub. An Ethernet hub is also known as a multiport repeater. Repeaters regenerate and retransmit communication signals. Notice that all intermediary devices perform the function of a repeater.

1.2.5 Network Media

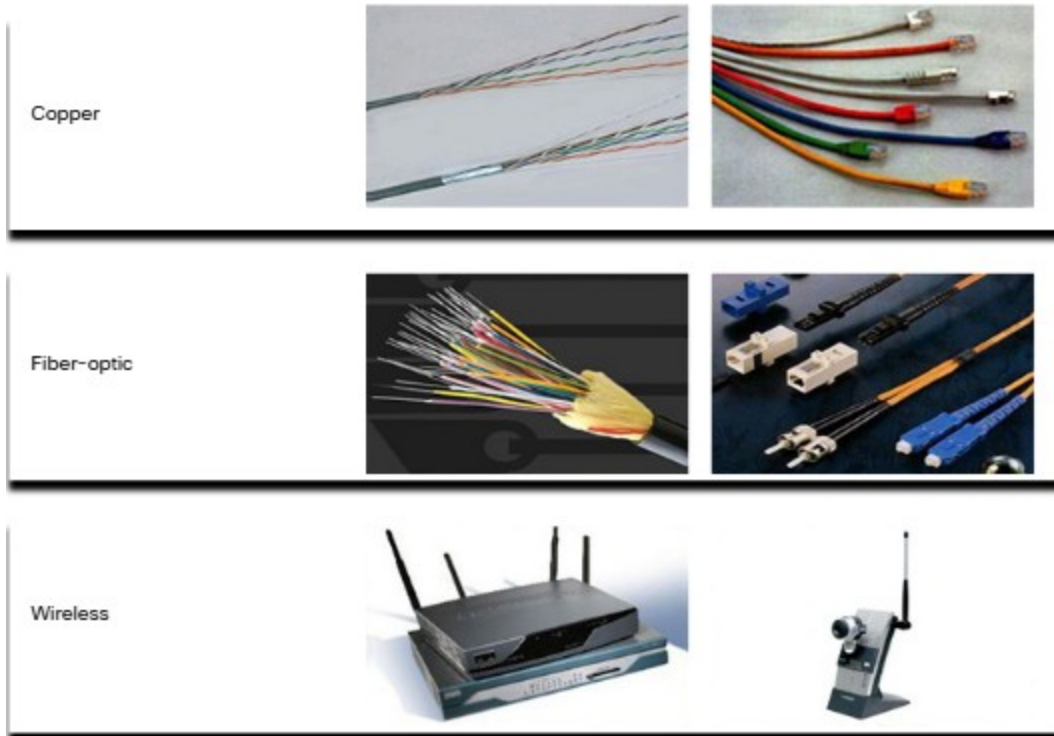
Communication transmits across a network on media. The media provides the channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices, as shown in the figure:

Metal wires within cables - Data is encoded into electrical impulses.

Glass or plastic fibers within cables (fiber-optic cable) - Data is encoded into pulses of light.

Wireless transmission - Data is encoded via modulation of specific frequencies of electromagnetic waves.



The four main criteria for choosing network media are these:

What is the maximum distance that the media can successfully carry a signal?

What is the environment in which the media will be installed?

What is the amount of data and at what speed must it be transmitted?

What is the cost of the media and installation?

1.2.6 Check Your Understanding - Network Components

Check your understanding of network components by choosing the BEST answer to the following questions.

Question 1

Which of the following is the name for all computers connected to a network that participate directly in network communication?

Servers

Intermediary devices

done Hosts

Media

Question 2

When data is encoded as pulses of light, which media is being used to transmit the data?

Wireless

done Fiber-optic cable

Copper cable

Question 3

Which two devices are intermediary devices? (Choose two)

Hosts

done

Routers

Servers

done Switches

100%

You've scored 100%.

Congratulations, you have passed the quiz!

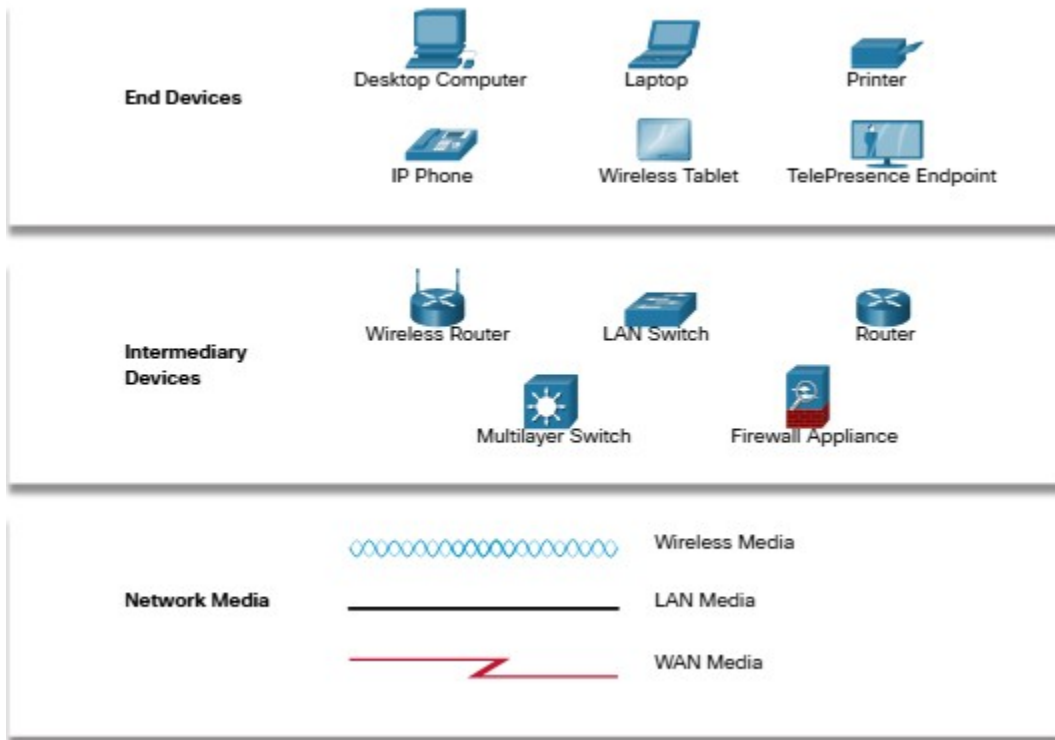
You've submitted your answers!

Reset

1.3 Network Representations and Topologies

1.3.1 Network Representations

Network architects and administrators must be able to show what their networks will look like. They need to be able to easily see which components connect to other components, where they will be located, and how they will be connected. Diagrams of networks often use symbols, like those shown in the figure, to represent the different devices and connections that make up a network.



A diagram provides an easy way to understand how devices connect in a large network. This type of “picture” of a network is known as a topology diagram. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network.

In addition to these representations, specialized terminology is used to describe how each of these devices and media connect to each other:

Network Interface Card (NIC) - A NIC physically connects the end device to the network.

Physical Port - A connector or outlet on a networking device where the media connects to an end device or another networking device.

Interface - Specialized ports on a networking device that connect to individual networks. Because routers connect networks, the ports on a router are referred to as network interfaces.

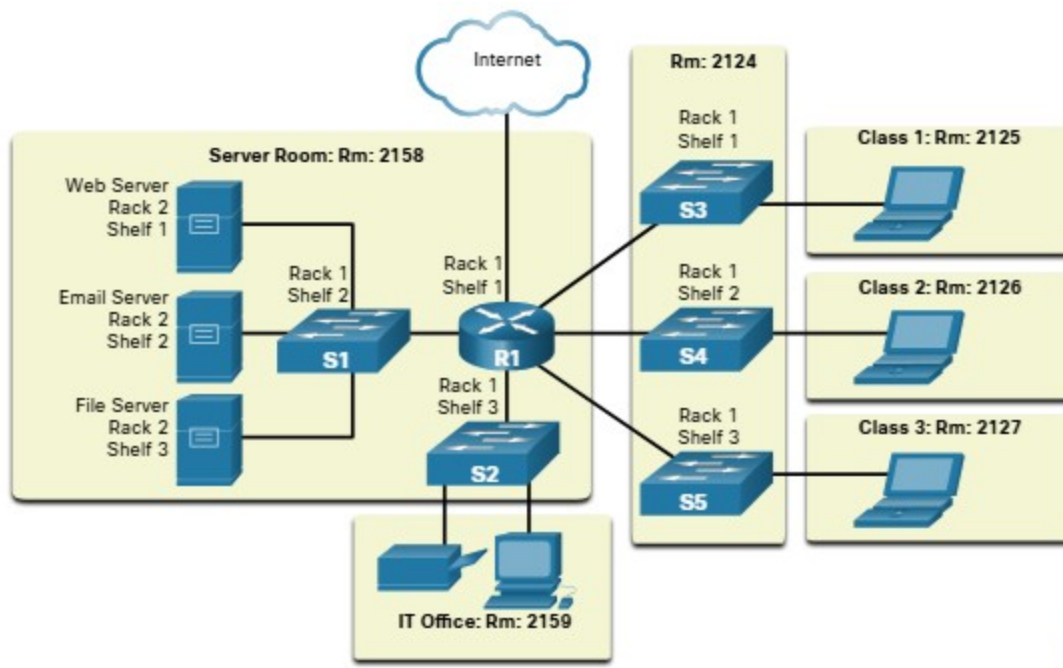
Note: The terms port and interface are often used interchangeably.

1.3.2 Topology Diagrams

Topology diagrams are mandatory documentation for anyone working with a network. They provide a visual map of how the network is connected. There are two types of topology diagrams: physical and logical.

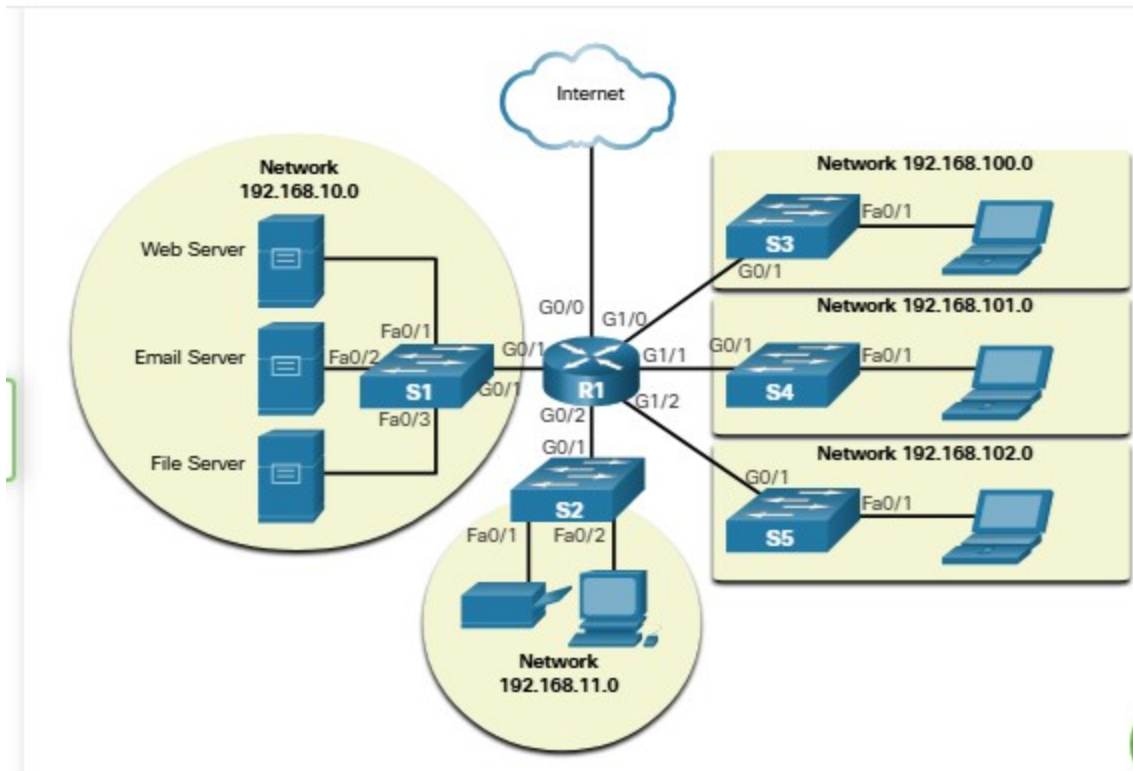
Physical Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation, as shown in the figure. You can see that the rooms in which these devices are located are labeled in this physical topology.



Logical Topology Diagrams

Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network, as shown in the figure. You can see which end devices are connected to which intermediary devices and what media is being used.



The topologies shown in the physical and logical diagrams are appropriate for your level of understanding at this point in the course. Search the internet for “network topology diagrams” to see some more complex examples. If you add the word “Cisco” to your search phrase, you will find many topologies using icons that are similar to what you have seen in these figures.

1.3.3 Check Your Understanding - Network Representations and Topologies

Check your understanding of network representations and topologies by choosing the BEST answer to the following questions.

Question 1

Which connection physically connects the end device to the network?

Port

done NIC

Question 2

Which connections are specialized ports on a networking device that connect to individual networks?

Port

NIC

done Interface

Question 3

Which type of network topology lets you see which end devices are connected to which intermediary devices and what media is being used?

Physical topology

done Logical topology

Question 4

Which type of network topology lets you see the actual location of intermediary devices and cable installation?

done Physical topology

Logical topology

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

reset

Interface

1.4 Common Types of Networks

1.4.1 Networks of Many Sizes

Now that you are familiar with the components that make up networks and their representations in physical and logical topologies, you are ready to learn about the many different types of networks.

Networks come in all sizes. They range from simple networks consisting of two computers, to networks connecting millions of devices.

Simple home networks let you share resources, such as printers, documents, pictures, and music, among a few local end devices.

Small office and home office (SOHO) networks allow people to work from home, or a remote office. Many self-employed workers use these types of networks to advertise and sell products, order supplies, and communicate with customers.

Businesses and large organizations use networks to provide consolidation, storage, and access to information on network servers. Networks provide email, instant messaging, and collaboration among employees. Many organizations use their network's connection to the internet to provide products and services to customers.

The internet is the largest network in existence. In fact, the term internet means a “network of networks”. It is a collection of interconnected private and public networks.

In small businesses and homes, many computers function as both the servers and clients on the network. This type of network is called a peer-to-peer network.

Click each button for more information.

Small Home Networks

Small home networks connect a few computers to each other and to the internet.



Small Office and Home Office Networks

The SOHO network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources.



Medium to Large Networks

Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts.



World Wide Networks

The internet is a network of networks that connects hundreds of millions of computers world-wide.



1.4.2 LANs and WANs

Network infrastructures vary greatly in terms of:

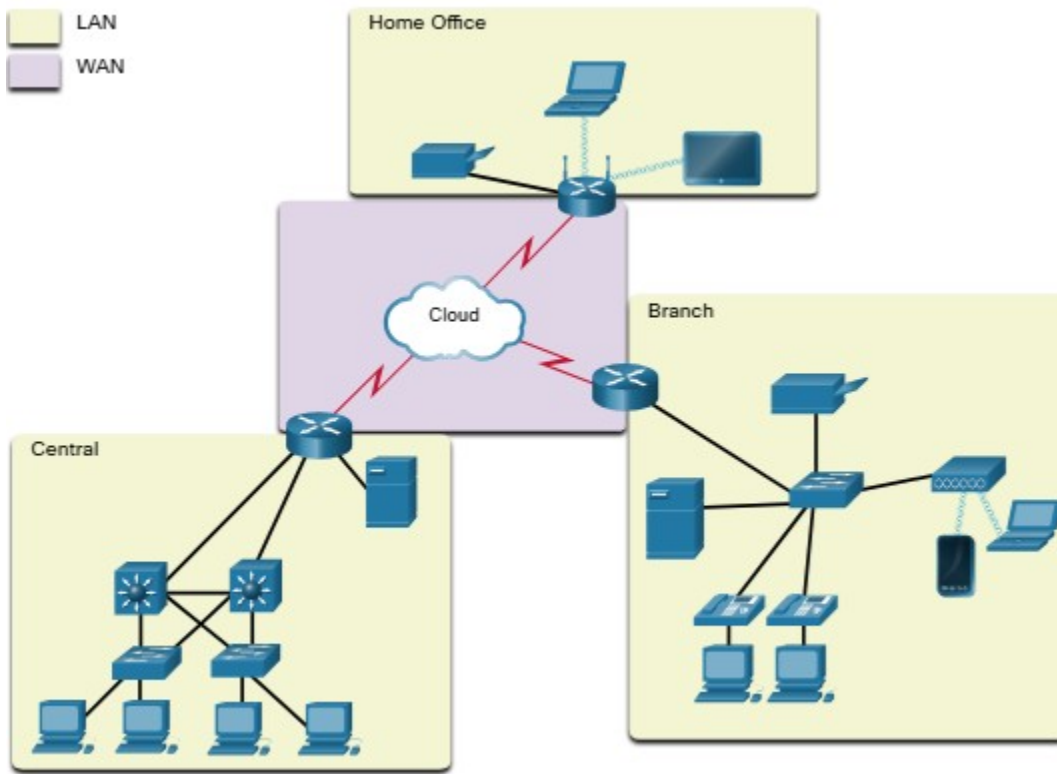
Size of the area covered

Number of users connected

Number and types of services available

Area of responsibility

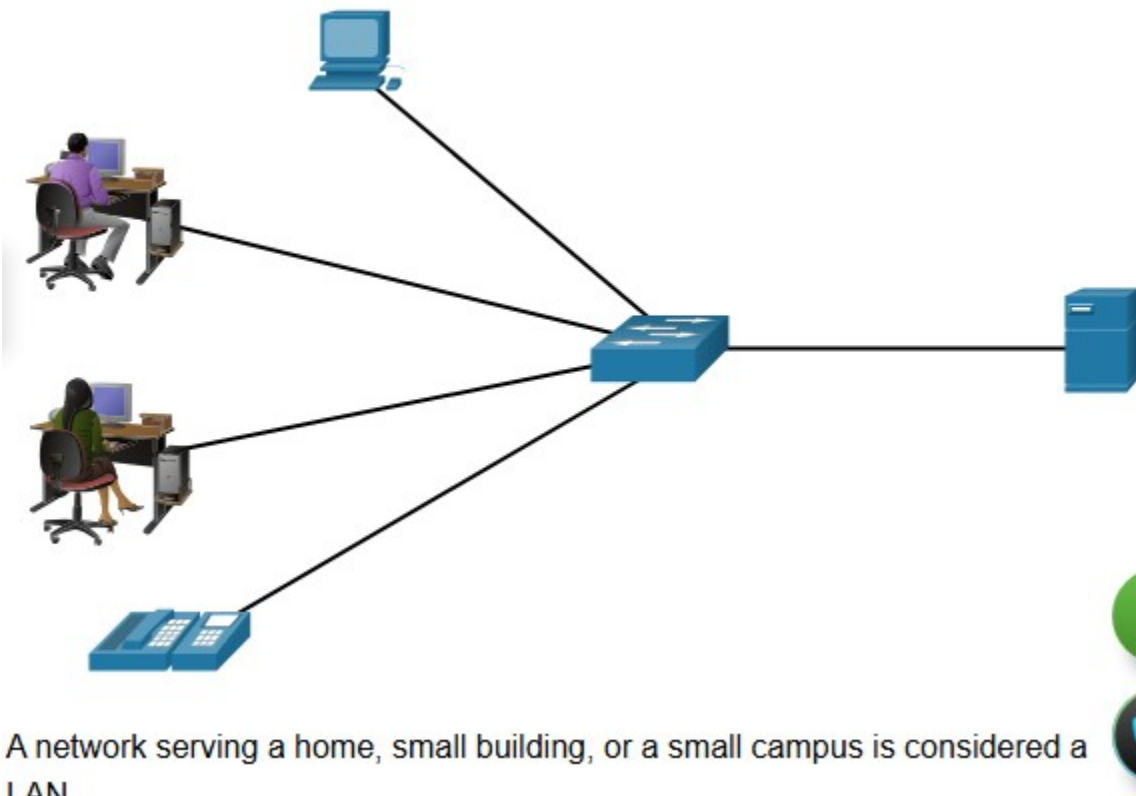
The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that provides access to users and end devices in a small geographical area. A LAN is typically used in a department within an enterprise, a home, or a small business network. A WAN is a network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a larger corporation or a telecommunications service provider. The figure shows LANs connected to a WAN.



LANs

A LAN is a network infrastructure that spans a small geographical area. LANs have specific characteristics:

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
- A LAN is usually administered by a single organization or individual. Administrative control is enforced at the network level and governs the security and access control policies.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices, as shown in the figure.



A network serving a home, small building, or a small campus is considered a LAN.

WANs

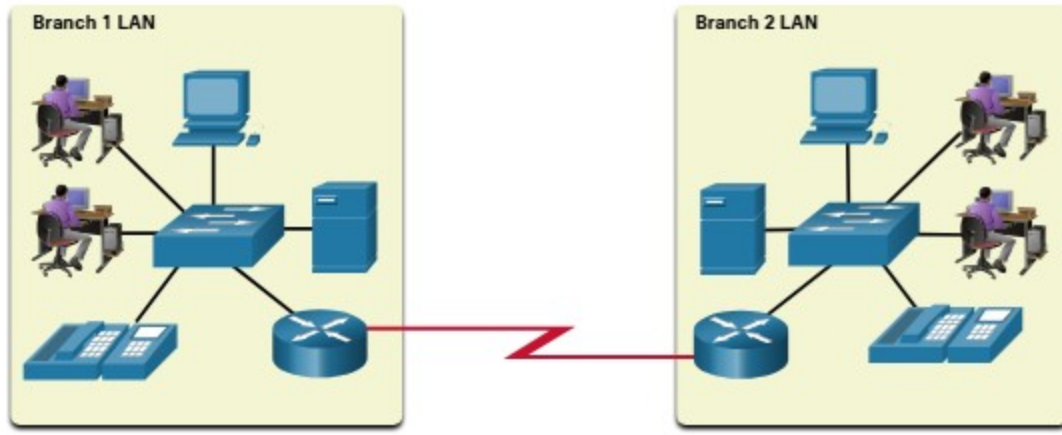
The figure shows a WAN which interconnects two LANs. A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.

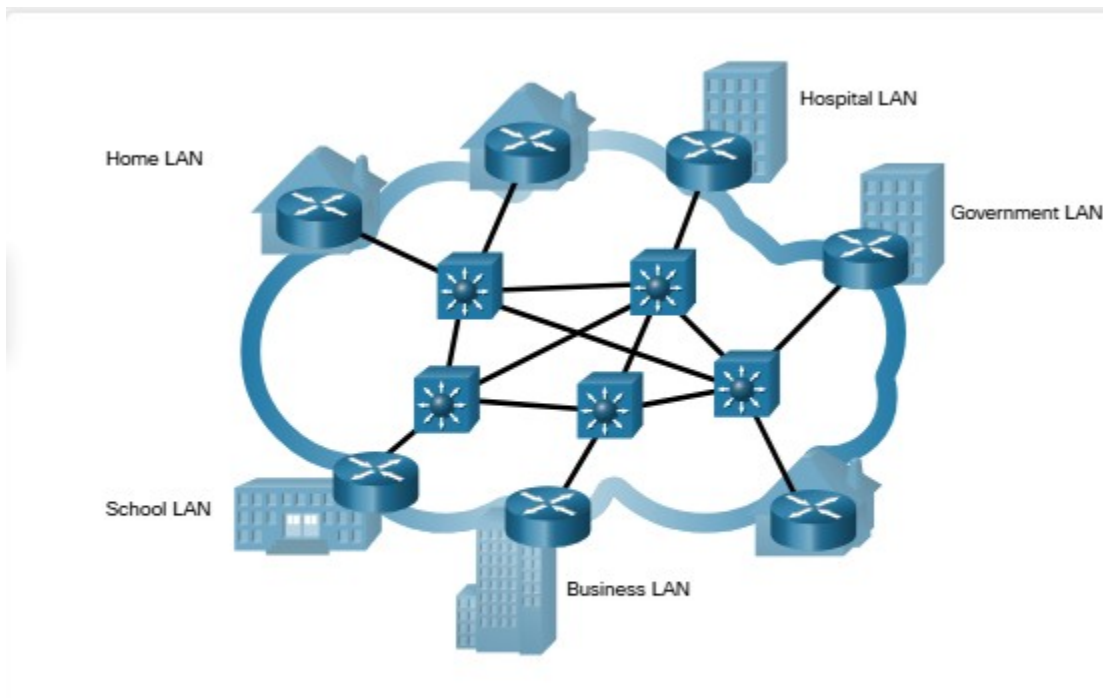
WANs are usually administered by multiple service providers.

WANs typically provide slower speed links between LANs.



1.4.3 The Internet

The internet is a worldwide collection of interconnected networks (internetworks, or internet for short). The figure shows one way to view the internet as a collection of interconnected LANs and WANs.



LANs use WAN services to interconnect.

Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions (not shown).

The internet is not owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that were developed to help maintain the structure and standardization of internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

1.4.4 Intranets and Extranets

There are two other terms which are similar to the term internet: intranet and extranet.

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization. An intranet is designed to be accessible only by the organization's members, employees, or others with authorization.

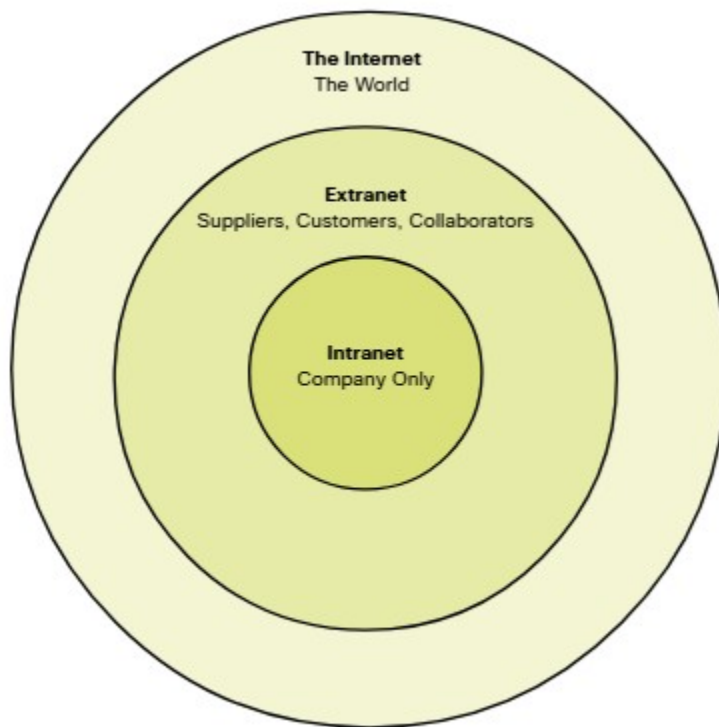
An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization's data. Here are some examples of extranets:

A company that is providing access to outside suppliers and contractors

A hospital that is providing a booking system to doctors so they can make appointments for their patients

A local office of education that is providing budget and personnel information to the schools in its district

The figure illustrates the levels of access that different groups have to a company intranet, a company extranet, and the internet.



1.4.5 Check Your Understanding - Common Types of Networks

Check your understanding of common types of networks by choosing the BEST answer to the following questions.

Question 1

Which network infrastructure provides access to users and end devices in a small geographical area, which is typically a network in a department in an enterprise, a home, or small business?

Extranet

Intranet

done

LAN

WAN

Question 2

Which network infrastructure might an organization use to provide secure and safe access to individuals who work for a different organization but require access to the organization's data?

done

Extranet

Intranet

LAN

WAN

Question 3

Which network infrastructure provides access to other networks over a large geographical area, which is often owned and managed by a telecommunications service provider?

Extranet

Intranet

LAN

done

WAN

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

[Reset](#)

1.5 Internet Connections

1.5.1 Internet Access Technologies

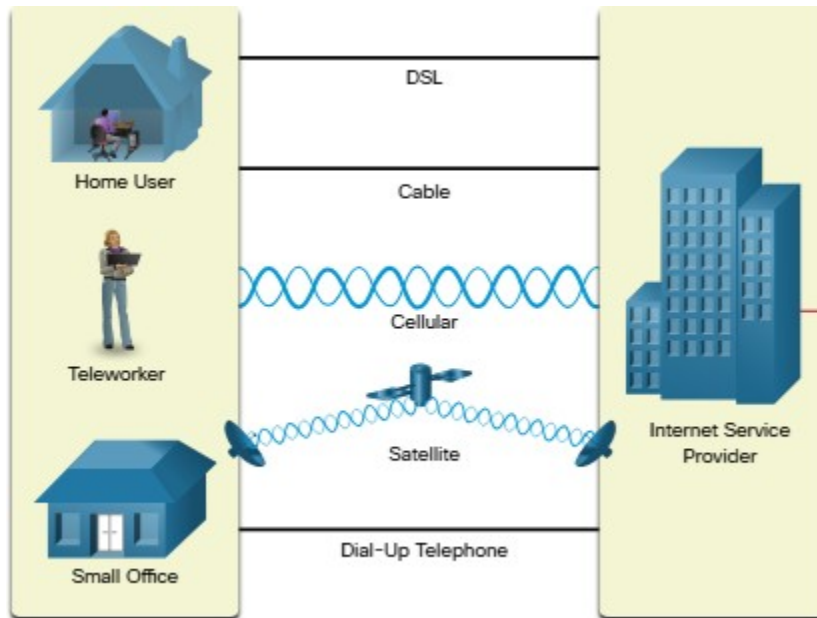
So, now you have a basic understanding of what makes up a network and the different types of networks. But, how do you actually connect users and organizations to the internet? As you may have guessed, there are many different ways to do this.

Home users, remote workers, and small offices typically require a connection to an ISP to access the internet. Connection options vary greatly between ISPs and geographical locations. However, popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations usually need access to other corporate sites as well as the internet. Fast connections are required to support business services including IP phones, video conferencing, and data center storage. SPs offer business-class interconnections. Popular business-class services include business DSL, leased lines, and Metro Ethernet.

1.5.2 Home and Small Office Internet Connections

The figure illustrates common connection options for small office and home office users.



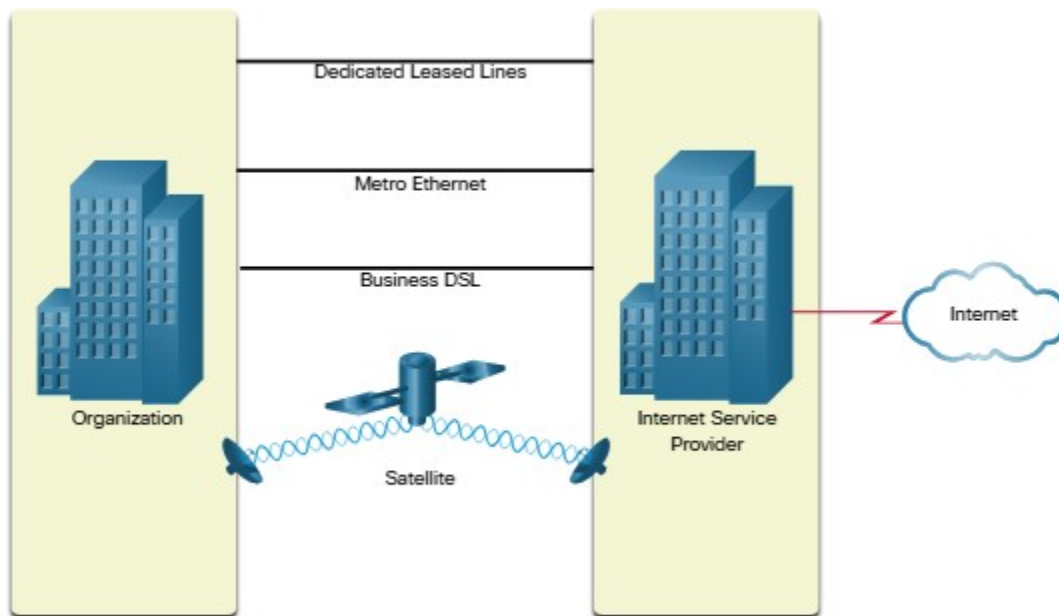
- **Cable** - Typically offered by cable television service providers, the internet data signal transmits on the same cable that delivers cable television. It provides a high bandwidth, high availability, and an always-on connection to the internet.
- **DSL** - Digital Subscriber Lines also provide high bandwidth, high availability, and an always-on connection to the internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
- **Cellular** - Cellular internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular internet access. Performance is limited by the capabilities of the phone and the cell tower to which it is connected.
- **Satellite** - The availability of satellite internet access is a benefit in those areas that would otherwise have no internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
- **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is not sufficient for large data transfer, although it is useful for mobile access while traveling.

The choice of connection varies depending on geographical location and service provider availability.

1.5.3 Businesses Internet Connections

Corporate connection options differ from home user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options that are available differ depending on the type of service providers located nearby.

The figure illustrates common connection options for businesses.



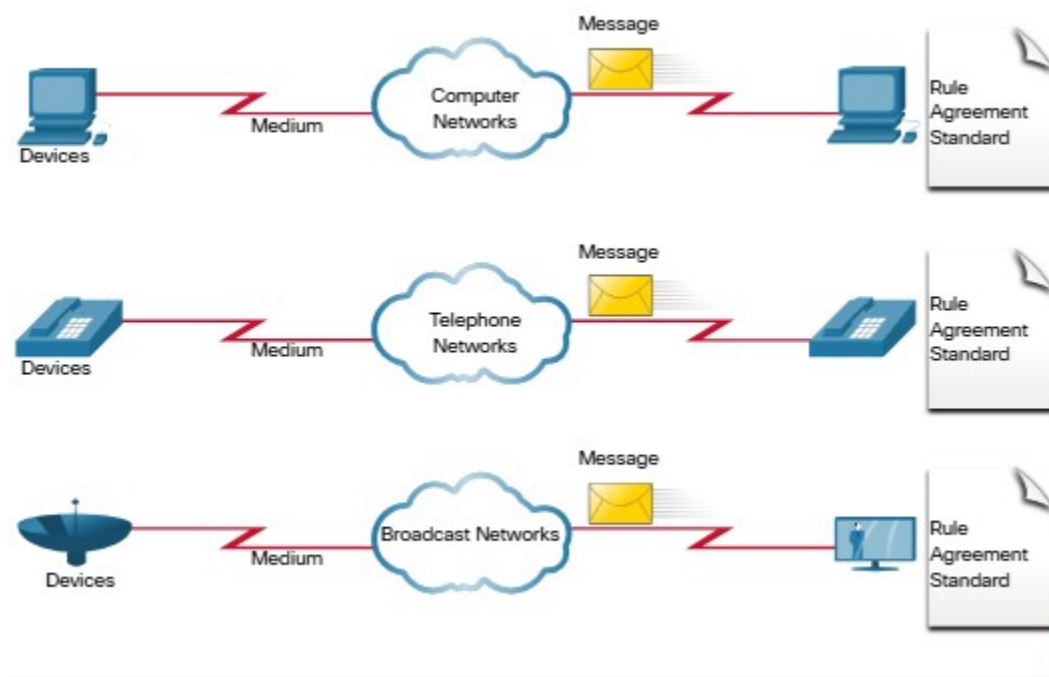
- **Dedicated Leased Line** - Leased lines are reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are rented at a monthly or yearly rate.
- **Metro Ethernet** - This is sometimes known as Ethernet WAN. In this module, we will refer to it as Metro Ethernet. Metro ethernets extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later module.
- **Business DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Line (SDSL) which is similar to the consumer version of DSL but provides uploads and downloads at the same high speeds.
- **Satellite** - Satellite service can provide a connection when a wired solution is not available.

The choice of connection varies depending on geographical location and service provider availability.

1.5.4 The Converging Network

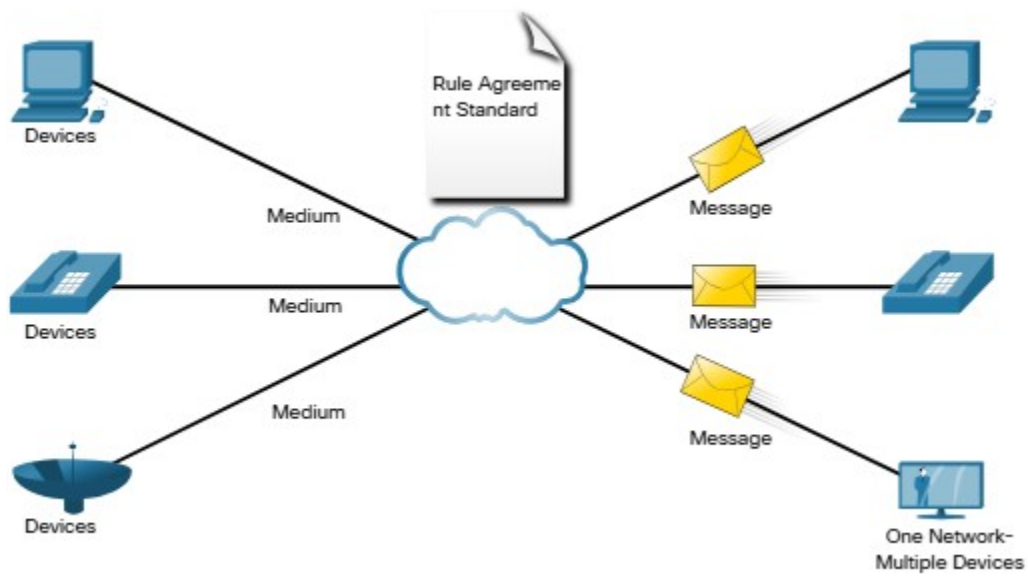
Traditional Separate Networks

Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other. Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication. Multiple services ran on multiple networks.



Converged Networks

Today, the separate data, telephone, and video networks converge. Unlike dedicated networks, converged networks are capable of delivering data, voice, and video between many different types of devices over the same network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards. Converged data networks carry multiple services on one network.



1.5.5 Packet Tracer - Network Representation

In this activity, you will explore how Packet Tracer serves as a modeling tool for network representations.

Description Network Representation file_download Network Representation

1.6 Reliable Networks

1.6.1 Network Architecture

Have you ever been busy working online, only to have “the internet go down”? As you know by now, the internet did not go down, you just lost your connection to it. It is very frustrating. With so many people in the world relying on network access to work and learn, it is imperative that networks are reliable. In this context, reliability means more than your connection to the internet. This topic focuses on the four aspects of network reliability.

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment. For networks to function efficiently and

grow in this type of environment, the network must be built upon a standard network architecture.

Networks also support a wide range of applications and services. They must operate over many different types of cables and devices, which make up the physical infrastructure. The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.

As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

Fault Tolerance

Scalability

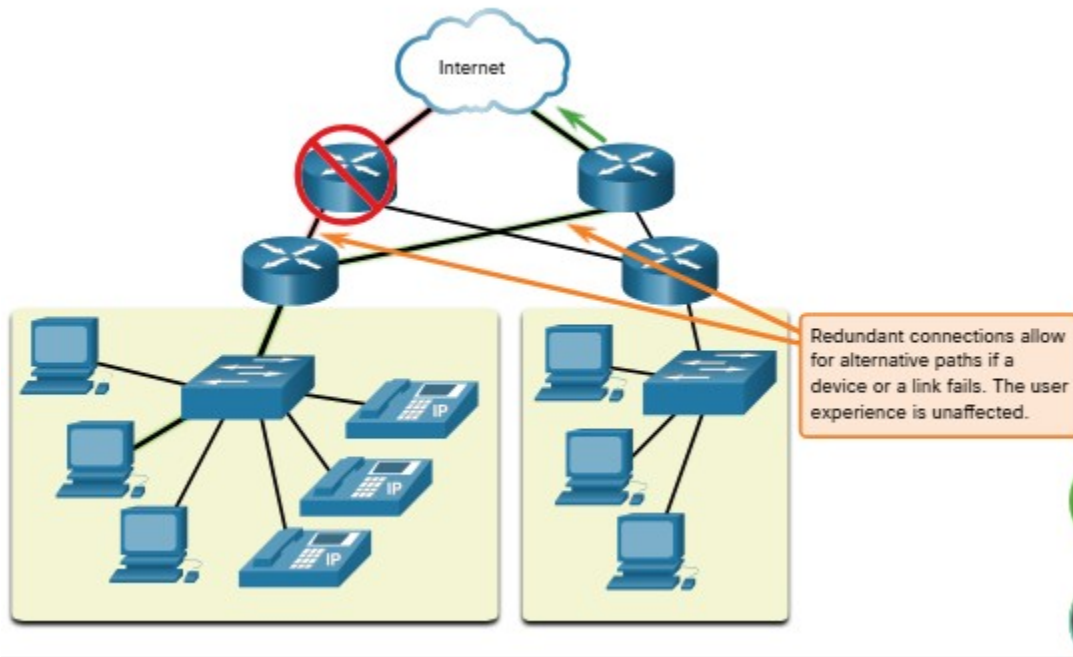
Quality of Service (QoS)

Security

1.6.2 Fault Tolerance

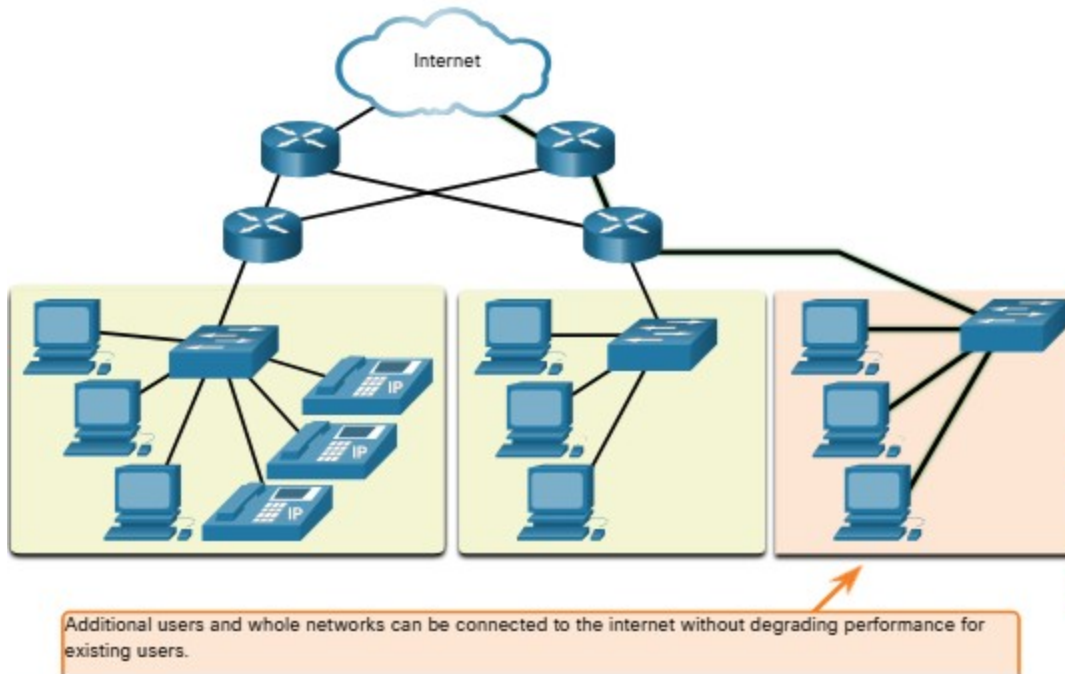
A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over a different link. Having multiple paths to a destination is known as redundancy.

Implementing a packet-switched network is one way that reliable networks provide redundancy. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the same destination. In the figure, the user is unaware and unaffected by the router that is dynamically changing the route when a link fails.



1.6.3 Scalability

A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

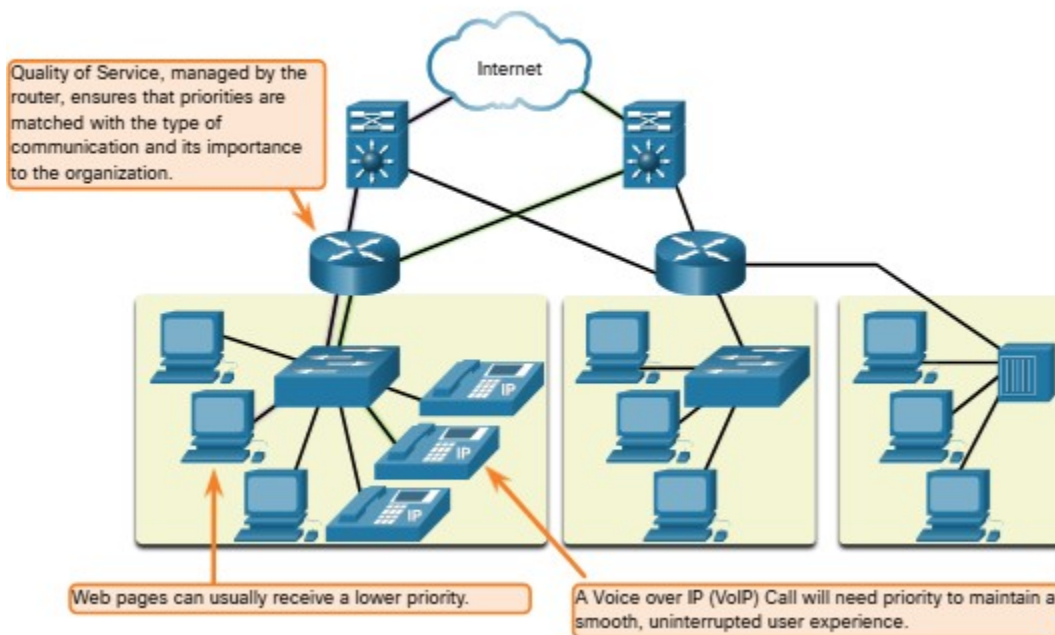


1.6.4 Quality of Service

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

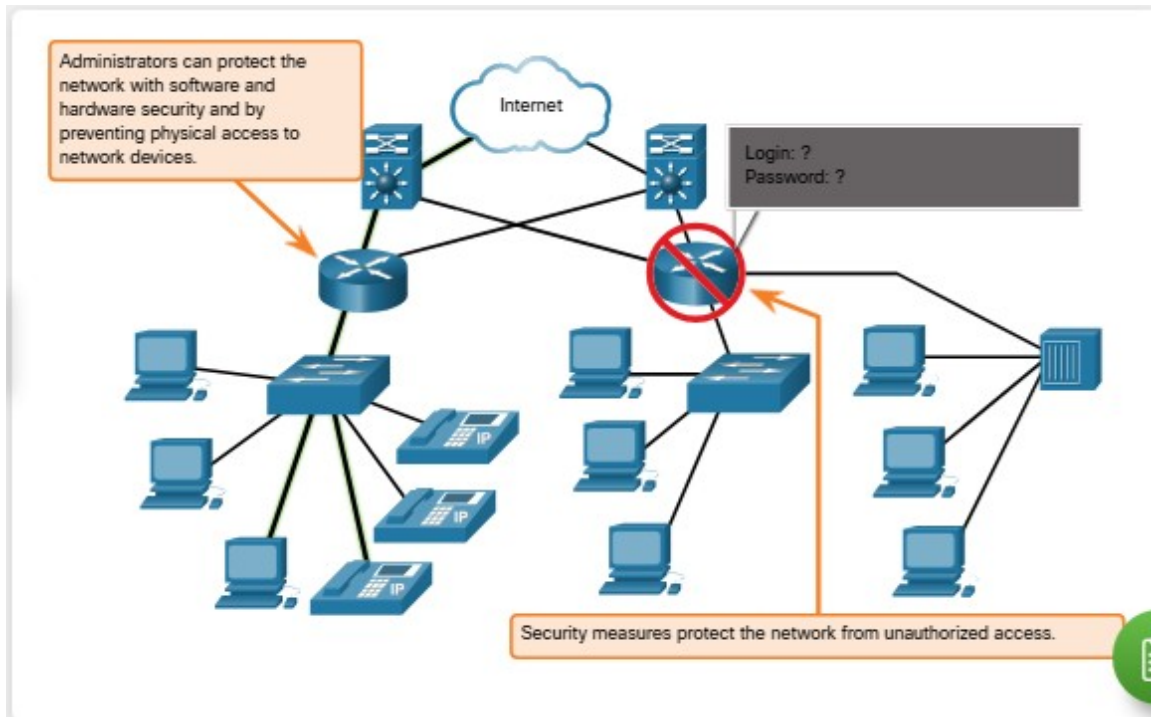
When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. In the figure, one user is requesting a web page, and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.



1.6.5 Network Security

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. Network administrators must address two types of network security concerns: network infrastructure security and information security.

Securing the network infrastructure includes physically securing devices that provide network connectivity and preventing unauthorized access to the management software that resides on them, as shown in the figure.



Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements.

Confidentiality - Data confidentiality means that only the intended and authorized recipients can access and read data.

Integrity - Data integrity assures users that the information has not been altered in transmission, from origin to destination.

Availability - Data availability assures users of timely and reliable access to data services for authorized users.

1.6.6 Check Your Understanding - Reliable Networks

Check your understanding of reliable networks by choosing the correct answer to the following questions.

Question 1

When designers follow accepted standards and protocols, which of the four basic characteristics of network architecture is achieved?

Fault tolerance

done

Scalability

QoS

Security

Question 2

Confidentiality, integrity, and availability are requirements of which of the four basic characteristics of network architecture?

Fault tolerance

Scalability

QoS

done

Security

Question 3

With which type of policy, a router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion?

Fault tolerance

Scalability

done

QoS

Security

Question 4

Having multiple paths to a destination is known as redundancy. This is an example of which characteristic of network architecture?

done

Fault tolerance

Scalability

QoS

Security

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

1.7 Network Trends

1.7.1 Recent Trends

You know a lot about networks now, what they are made of, how they connect us, and what is needed to keep them reliable. But networks, like everything else, continue to change. There are a few trends in networking that you, as a NetAcad student, should know about.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several networking trends that affect organizations and consumers:

Bring Your Own Device (BYOD)

Online collaboration

Video communications

Cloud Computing

1.7.2 Bring Your Own Device (BYOD)

The concept of any device, for any content, in any manner, is a major global trend that requires significant changes to the way we use devices and safely connect them to networks. This is called Bring Your Own Device (BYOD).

BYOD enables end users the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students may have advanced computing and networking devices for personal use. These include laptops, notebooks, tablets, smart phones, and e-readers. These may be purchased by the company or school, purchased by the individual, or both.

BYOD means any device, with any ownership, used anywhere.



1.7.3 Online Collaboration

Individuals want to connect to the network, not only for access to data applications, but also to collaborate with one another. Collaboration is defined as “the act of working with another or others on a joint project.” Collaboration tools, like Cisco WebEx, shown in the figure, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.



Collaboration is a critical and strategic priority that organizations are using to remain competitive. Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop the team skills used in the workforce, and to work together on team-based projects.

Cisco Webex Teams is a multifunctional collaboration tool that lets you send instant messages to one or more people, post images, and post videos and links. Each team 'space' maintains a history of everything that is posted there.

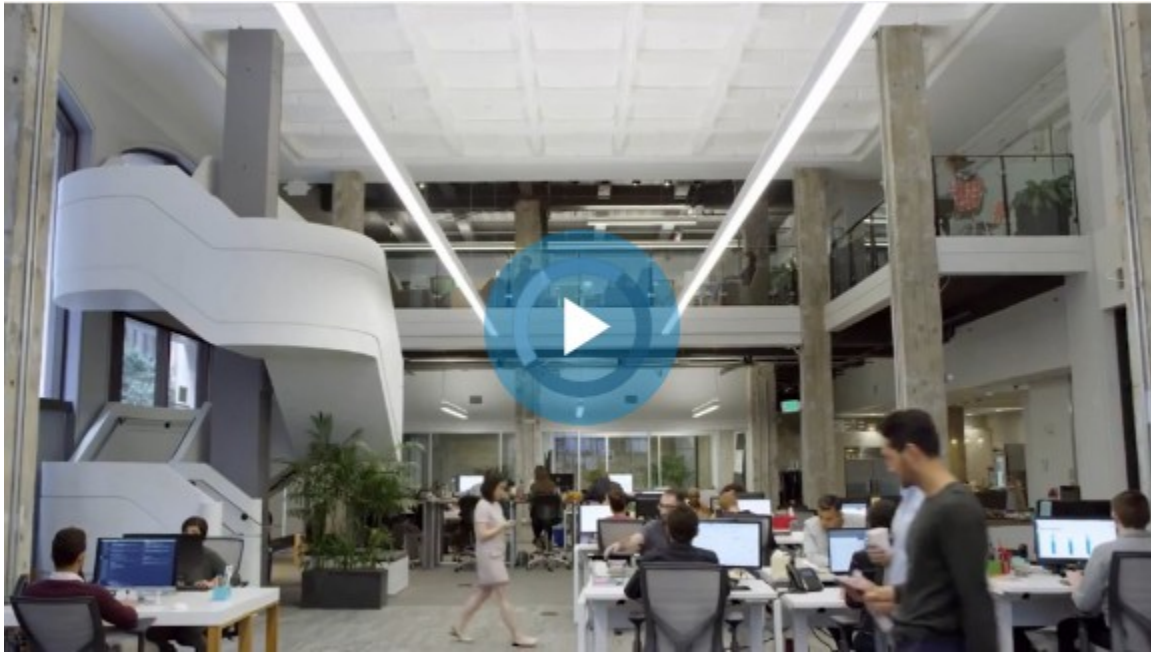
1.7.4 Video Communications

Another facet of networking that is critical to the communication and collaboration effort is video. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located.

Video conferencing is a powerful tool for communicating with others, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries.

1.7.5 Video - Cisco Webex for Huddles

Click Play in the figure to view how Cisco Webex is incorporated into everyday life and business.



Transcript

Follow along using the transcript.
ShowTranscript

Transcript

16px (default)

English

- 00:00(upbeat music)
- 00:01- Hello.
- 00:02Hello.
- 00:03You're going to have to call me back.
- 00:04(crowd chattering)
- 00:08(upbeat music)
- 00:10- Did you guys book this room?
- 00:11'Cause I'm pretty sure I booked this room.
- 00:13(upbeat music)

1.7.6 Cloud Computing

Cloud computing is one of the ways that we access and store data. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud.

For businesses, Cloud computing extends the capabilities of IT without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on-demand and delivered economically to any device that is anywhere in the world without compromising security or function.

Cloud computing is possible because of data centers. Data centers are facilities used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire warehouse-sized building. Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

For security, reliability, and fault tolerance, cloud providers often store data in distributed data centers. Instead of storing all the data of a person or an organization in one data center, it is stored in multiple data centers in different locations.

There are four primary types of clouds: Public clouds, Private clouds, Hybrid clouds, and Community clouds, as shown in the table.

Cloud Types

Cloud Type Description

Public clouds Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the internet to provide services.

Private clouds Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as a government. A private cloud can be set up using the organization's private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.

Hybrid clouds A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a distinct object, but both are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.

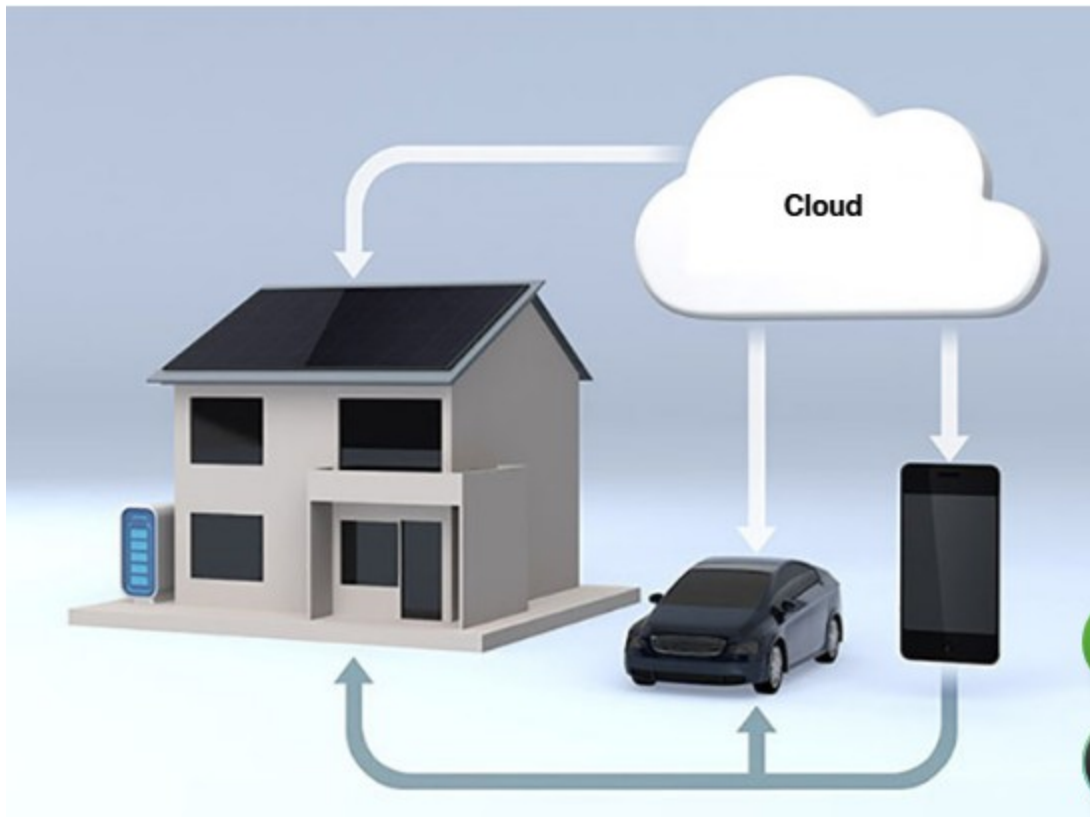
Community clouds A community cloud is created for exclusive use by specific entities or organizations. The differences between public clouds and community clouds are the functional needs that have been customized for the community. For example, healthcare organizations must remain compliant with policies and laws (e.g. HIPAA) that require special authentication and confidentiality. Community clouds are used by multiple organizations that have similar needs and concerns. Community clouds are similar to a public cloud environment, but with set levels of security, privacy, and even regulatory compliance of a private cloud.

1.7.7 Technology Trends in the Home

Networking trends are not only affecting the way we communicate at work and at school, but also changing many aspects of the home. The newest home trends include 'smart home technology'.

Smart home technology integrates into every-day appliances, which can then connect with other devices to make the appliances more 'smart' or automated. For example, you could prepare food and place it in the oven for cooking prior to leaving the house for the day. You program your smart oven for the food you want it to cook. It would also be connected to your 'calendar of events' so that it could determine what time you should be available to eat and adjust start times and length of cooking accordingly. It could even adjust cooking times and temperatures based on changes in schedule. Additionally, a smart phone or tablet connection lets you connect to the oven directly, to make any desired adjustments. When the food is ready, the oven sends an alert message to you (or someone you specify) that the food is done and warming.

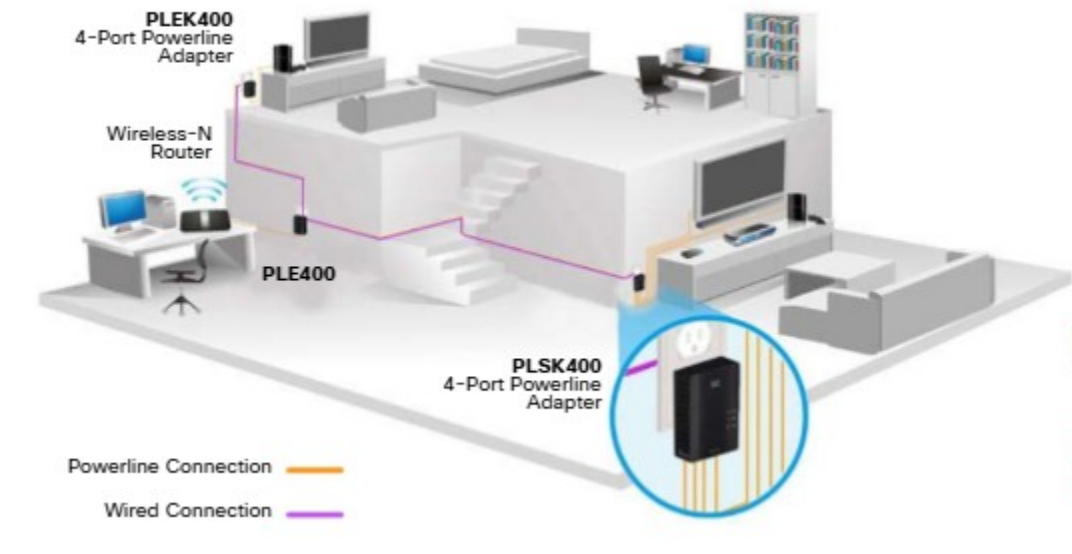
Smart home technology is currently being developed for all rooms within a house. Smart home technology will become more common as home networking and high-speed internet technology expands.



The smart phone is updated from the cloud with the status of the smart home devices and the smart car. The user can then use the smart phone to interact with the smart home and smart car.

1.7.8 Powerline Networking

Powerline networking for home networks uses existing electrical wiring to connect devices, as shown in the figure.



Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. No data cables need to be installed, and there is little to no additional electricity used. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

Powerline networking is especially useful when wireless access points cannot reach all the devices in the home. Powerline networking is not a substitute for dedicated cabling in data networks. However, it is an alternative when data network cables or wireless communications are not possible or effective.

1.7.9 Wireless Broadband

In many areas where cable and DSL are not available, wireless may be used to connect to the internet.

Wireless Internet Service Provider

A Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower may be installed for the antenna, typically the antenna is attached to an existing elevated structure, such as a water tower or a radio tower. A small dish or antenna is installed on the subscriber's roof in range of the WISP transmitter. The subscriber's access unit is connected to the wired network inside the home. From the perspective of the home user, the setup is not much different than DSL or cable service. The main difference is that the connection from the home to the ISP is wireless instead of a physical cable.

Wireless Broadband Service

Another wireless solution for the home and small businesses is wireless broadband, as shown in the figure.



This solution uses the same cellular technology as a smart phone. An antenna is installed outside the house providing either wireless or wired connectivity

for devices in the home. In many areas, home wireless broadband is competing directly with DSL and cable services.

1.7.10 Check Your Understanding - Network Trends

Check your understanding of network trends by choosing the BEST answer to the following questions.

Question 1

Which feature is a good conferencing tool to use with others who are located elsewhere in your city, or even in another country?

BYOD

done

Video communications

Cloud computing

Question 2

Which feature describes using personal tools to access information and communicate across a business or campus network?

done

BYOD

Video communications

Cloud computing

Question 3

Which feature contains options such as Public, Private, Custom and Hybrid?

BYOD

Video communications

done

Cloud computing

Question 4

Which feature is being used when connecting a device to the network using an electrical outlet?

Smart home technology

done

Powerline

Wireless broadband

Question 5

Which feature uses the same cellular technology as a smartphone?

Smart home technology

Powerline

done

Wireless broadband

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

1.8 Network Security

1.8.1 Security Threats

You have, no doubt, heard or read news stories about a company network being breached, giving threat actors access to the personal information of thousands of customers. For this reason, network security is always going to be a top priority of administrators.

Network security is an integral part of computer networking, regardless of whether the network is in a home with a single connection to the internet or is a corporation with thousands of users. Network security must consider the environment, as well as the tools and requirements of the network. It must be able to secure data while still allowing for the quality of service that users expect of the network.

Securing a network involves protocols, technologies, devices, tools, and techniques in order to protect data and mitigate threats. Threat vectors may be external or internal. Many external network security threats today originate from the internet.

There are several common external threats to networks:

Viruses, worms, and Trojan horses - These contain malicious software or code running on a user device.

Spyware and adware - These are types of software which are installed on a user's device. The software then secretly collects information about the user.

Zero-day attacks - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.

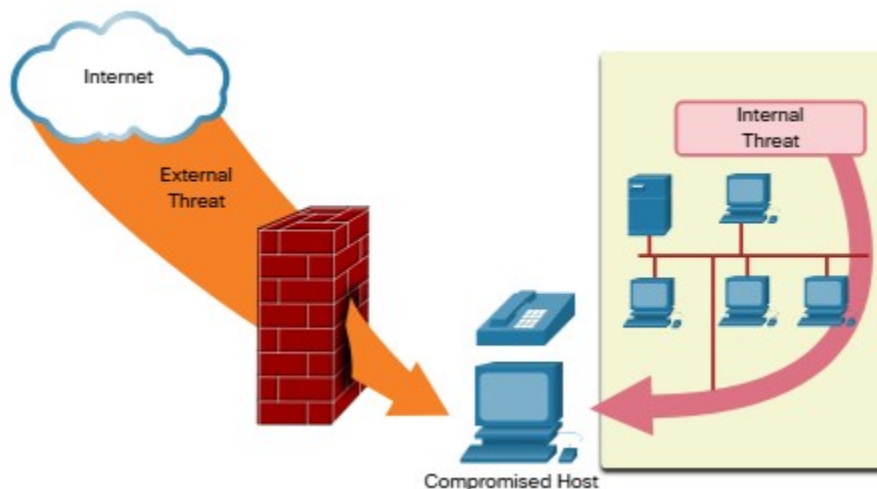
Threat actor attacks - A malicious person attacks user devices or network resources.

Denial of service attacks - These attacks slow or crash applications and processes on a network device.

Data interception and theft - This attack captures private information from an organization's network.

Identity theft - This attack steals the login credentials of a user in order to access private data.

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats, as shown in the figure.



1.8.2 Security Solutions

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others may succeed.

A home network security implementation is usually rather basic. Typically, you implement it on the end devices, as well as at the point of connection to the internet, and can even rely on contracted services from the ISP.

These are the basic security components for a home or small office network:

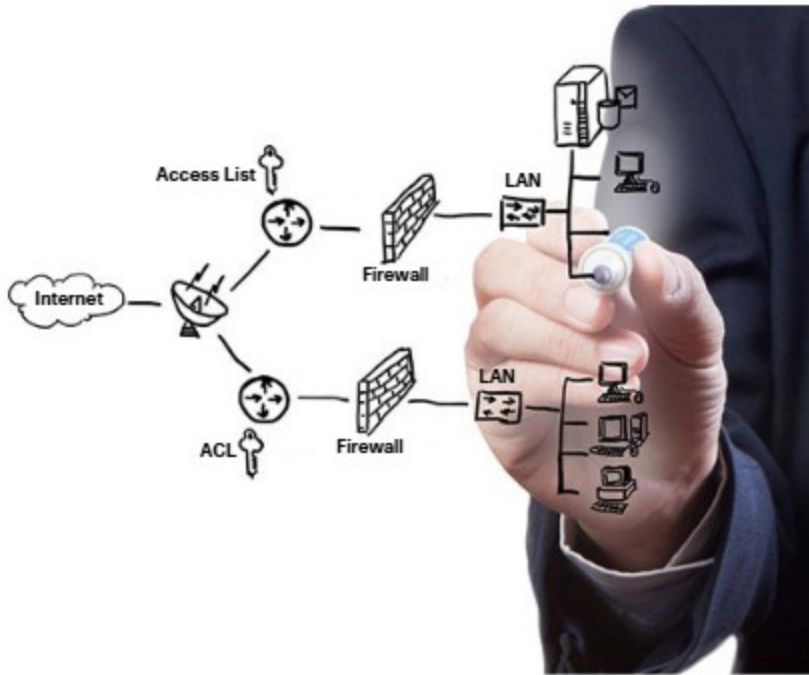
- **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
- **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In contrast, the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security. Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- **Dedicated firewall systems** - These provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL)** - These further filter access and traffic forwarding based on IP addresses and applications.
- **Intrusion prevention systems (IPS)** - These identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN)** - These provide secure access into an organization for remote workers.

Network security requirements must consider the environment, as well as the various applications, and computing requirements. Both home and business environments must be able to secure their data while still allowing for the quality of service that users expect of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.



1.8.3 Check Your Understanding - Network Security

Check your understanding of network security by choosing the BEST answer to the following questions.

Question 1

Which attack slows down or crashes equipment and programs?

Firewall

Virus, worm, or Trojan horse

Zero-day or Zero-hour

Virtual Private Network (VPN)

done

Denial of Service (DoS)

Question 2

Which option creates a secure connection for remote workers?

Firewall

Virus, worm, or Trojan horse

Zero-day or Zero-hour

done

Virtual Private Network (VPN)

Denial of Service (DoS)

Question 3

Which option blocks unauthorized access to your network?

done

Firewall

Virus, worm, or Trojan horse

Zero-day or Zero-hour

Virtual Private Network (VPN)

Denial of Service (DoS)

Question 4

Which option describes a network attack that occurs on the first day that a vulnerability becomes known?

Firewall

Virus, worm, or Trojan horse

done

Zero-day or Zero-hour

Virtual Private Network (VPN)

Denial of Service (DoS)

Question 5

Which option describes malicious code running on user devices?

Firewall

done

Virus, worm, or Trojan horse

Zero-day or Zero-hour

Virtual Private Network (VPN)

Denial of Service (DoS)

100%

You've scored 100%.

Congratulations, you have passed the quiz!

You've submitted your answers!

Reset

1.9 The IT Professional

1.9.1 CCNA

As a NetAcad student, you may already have a career in IT, or are still educating yourself to prepare for your career. In either case, it is good to know about the skills needed to match the types of jobs that are available in IT.

The role and skills required of network engineers are evolving and are more vital than ever. The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures you stay relevant with skill sets needed for the adoption of next-generation technologies.

A consolidated and updated CCNA for networking engineers is three courses and one exam which covers the fundamental topics for all network technologies. The new CCNA focuses on IP foundation and security topics along with wireless, virtualization, automation, and network programmability.

There are new DevNet certifications at the associate, specialist and professional levels, to validate your software development skills.

There are specialist certification options to validate your skills in line with your job role and interests. This includes the Cisco Enterprise Advanced Infrastructure Specialist certification.

You can start where you want. There are no prerequisites to start earning your associate, specialist, professional, or expert level certification. Continuing education credits for recertification and ongoing development are now available for CCNA.

1.9.2 Networking Jobs

Your CCNA certification will prepare you for a variety of jobs in today's market. At www.netacad.com you can click the Careers menu and then select Employment opportunities. You can find employment opportunities where you live by using the new program, the Talent Bridge Matching Engine. Search for jobs with Cisco, as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

You can also search for IT jobs using online search engines such as Indeed, Glassdoor, and Monster. Use search terms such as IT, network administrator, network architects, and computer systems administrator. You can also search using the term Cisco CCNA.

1.9.3 Lab - Research IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

Part 1: Research Job Opportunities

Part 2: Reflect on Research

description

Research IT and Networking Job Opportunities

1.10 Module Practice and Quiz

1.10.1 What did I learn in this module?

Networks Affect our Lives

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe. The creation of the cloud lets us store documents and pictures and access them anywhere, anytime.

Network Components

All computers that are connected to a network and participate directly in network communication are classified as hosts. Hosts can be called end

devices. Some hosts are also called clients. Many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network. An end device is either the source or destination of a message transmitted over the network. Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network. The media provides the channel over which the message travels from source to destination.

Network Representations and Topologies

Diagrams of networks often use symbols to represent the different devices and connections that make up a network. A diagram provides an easy way to understand how devices connect in a large network. This type of “picture” of a network is known as a topology diagram. Physical topology diagrams illustrate the physical location of intermediary devices and cable installation. Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.

Common Types of Networks

Small home networks connect a few computers to each other and to the internet. The small office/home office (SOHO) network allows computers in a home office or a remote office to connect to a corporate network, or access centralized, shared resources. Medium to large networks, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected hosts. The internet is a network of networks that connects hundreds of millions of computers world-wide. The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that spans a small geographical area. A WAN is a network infrastructure that spans a wide geographical area. Intranet refers to a private connection of LANs and WANs that belongs to an organization. An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization’s data.

Internet Connections

SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone. Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite. The choice of connection varies depending on geographical location and service provider availability. Traditional separate networks used different technologies, rules, and standards. Converged networks deliver data, voice, and video between many

different types of devices over the same network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards. Packet Tracer is a flexible software program that lets you use network representations and theories to build network models and explore relatively complex LANs and WANs.

Reliable Networks

The term network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network. As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations: Fault Tolerance, Scalability, Quality of Service (QoS), and Security. A fault tolerant network is one that limits the number of affected devices during a failure. Having multiple paths to a destination is known as redundancy. A scalable network expands quickly to support new users and applications. Networks are scalable because the designers follow accepted standards and protocols. QoS is a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network administrators must address two types of network security concerns: network infrastructure security and information security. To achieve the goals of network security, there are three primary requirements: Confidentiality, Integrity, and Availability.

Network Trends

There are several recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing. BYOD means any device, with any ownership, used anywhere. Collaboration tools, like Cisco WebEx give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud. There are four primary types of Clouds: Public Clouds, Private Clouds, Hybrid Clouds, and Custom Clouds. Smart home technology is currently being developed for all rooms within a house. Smart home technology will become more common as home networking and high-speed internet technology expands. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies. A Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot

spot using similar wireless technologies found in home wireless local area networks (WLANs).

Network Security

There are several common external threats to networks:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

These are the basic security components for a home or small office network:

- Antivirus and antispyware
- Firewall filtering

Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

- Dedicated firewall systems
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The IT Professional

The Cisco Certified Network Associate (CCNA) certification demonstrates that you have a knowledge of foundational technologies and ensures you stay relevant with skill sets needed for the adoption of next-generation technologies. Your CCNA certification will prepare you for a variety of jobs in today's market. At www.netacad.com you can click the Careers menu and then select Employment opportunities. You can find employment opportunities where you live by using the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni.

1.10.2 Module Quiz – Networking Today

Question 1

During a routine inspection, a technician discovered that software that was installed on a computer was secretly collecting data about websites that were visited by users of the computer. Which type of threat is affecting this computer?

DoS attack

identity theft

spyware

zero-day attack

Explanation: Spyware is software that is installed on a network device and that collects information.

Question 2

Which term refers to a network that provides secure access to the corporate offices by suppliers, customers and collaborators?

Internet

intranet

extranet

extendednet

Explanation: The term Internet refers to the worldwide collection of connected networks. Intranet refers to a private connection of LANs and WANS that belong to an organization and is designed to be accessible to the members of the organization, employees, or others with authorization. Extranets provide secure and safe access to suppliers, customers, and collaborators. Extendednet is not a type of network.

Question 3

A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

cloud computing

online collaboration

bring your own device

video conferencing

Explanation: BYOD allows end users to use personal tools to access the corporate network. Allowing this trend can have major impacts on a network, such as security and compatibility with corporate software and devices.

Question 4

What is an ISP?

It is a standards body that develops cabling and wiring standards for networking.

It is a protocol that establishes how computers within a local network communicate.

It is an organization that enables individuals and businesses to connect to the Internet.

It is a networking device that combines the functionality of several different networking devices in one.

Explanation: An ISP, or Internet Service Provider, is an organization that provides access to the Internet for businesses and individuals.

Question 5

In which scenario would the use of a WISP be recommended?

an Internet cafe in a city

a farm in a rural area without wired broadband access

any home with multiple wireless devices

an apartment in a building with cable access to the Internet

Explanation: Wireless Internet Service Providers (WISPs) are typically found in rural areas where DSL or cable access is not available. A dish or antenna on the property of the subscriber connects wirelessly to a WISP transmitter, eliminating the need for physical cabling outside the building.

Question 6

What characteristic of a network enables it to quickly grow to support new users and applications without impacting the performance of the service being delivered to existing users?

reliability

scalability

quality of service

accessibility

Explanation: Networks must be able to quickly grow to support new users and services, without impacting existing users and services. This ability to grow is known as scalability.

Question 7

A college is building a new dormitory on its campus. Workers are digging in the ground to install a new water pipe for the dormitory. A worker accidentally damages a fiber optic cable that connects two of the existing dormitories to the campus data center. Although the cable has been cut, students in the dormitories only experience a very short interruption of network services. What characteristic of the network is shown here?

quality of service (QoS)

scalability

security

fault tolerance

integrity

Explanation: Fault tolerance is the characteristic of a network which allows it to quickly respond to failures of network devices, media, or services. Quality of service refers to the measures taken to ensure that network traffic requiring higher throughput receives the required network resources. Scalability refers to the ability of the network to grow to accommodate new requirements. Security refers to protecting networks and data from theft, alteration, or destruction. Integrity refers to the completeness of something and is generally not used as a characteristic of networks in the same way as the other terms.

Question 8

What are two characteristics of a scalable network? (Choose two.)

easily overloaded with increased traffic

grows in size without impacting existing users

is not as reliable as a small network

suitable for modular devices that allow for expansion

offers limited number of applications

Explanation: Scalable networks are networks that can grow without requiring costly replacement of existing network devices. One way to make a network scalable is to buy networking devices that are modular.

Question 9

Which device performs the function of determining the path that messages should take through internetworks?

a router

a firewall

a web server

a DSL modem

Explanation: A router is used to determine the path that the messages should take through the network. A firewall is used to filter incoming and outgoing traffic. A DSL modem is used to provide Internet connection for a home or an organization.

Question 10

Which two Internet connection options do not require that physical cables be run to the building? (Choose two.)

DSL

cellular

satellite

dialup

dedicated leased line

Explanation: Cellular connectivity requires the use of the cell phone network. Satellite connectivity is often used where physical cabling is not available outside the home or business.

Question 11

What type of network must a home user access in order to do online shopping?

an intranet

the Internet

an extranet

a local area network

Explanation: Home users will go online shopping over the Internet because online vendors are accessed through the Internet. An intranet is basically a local area network for internal use only. An extranet is a network for external partners to access certain resources inside an organization. A home user does not necessarily need a LAN to access the Internet. For example, a PC connects directly to the ISP through a modem.

Question 12

How does BYOD change the way in which businesses implement networks?

BYOD requires organizations to purchase laptops rather than desktops.

BYOD users are responsible for their own network security, thus reducing the need for organizational security policies.

BYOD devices are more expensive than devices that are purchased by an organization.

BYOD provides flexibility in where and how users can access network resources.

Explanation: A BYOD environment requires an organization to accommodate a variety of devices and access methods. Personal devices, which are not under company control, may be involved, so security is critical. Onsite hardware costs will be reduced, allowing a business to focus on delivering collaboration tools and other software to BYOD users.

Question 13

An employee wants to access the network of the organization remotely, in the safest possible way. What network feature would allow an employee to gain secure remote access to a company network?

ACL

IPS

VPN

BYOD

Explanation: Virtual private networks (VPN) are used to provide secure access to remote workers.

Question 14

What is the Internet?

It is a network based on Ethernet technology.

It provides network access for mobile devices.

It provides connections through interconnected global networks.

It is a private network for an organization with LAN and WAN connections.

Explanation: The Internet provides global connections that enable networked devices (workstations and mobile devices) with different network technologies, such as Ethernet, DSL/cable, and serial connections, to communicate. A private network for an organization with LAN and WAN connections is an intranet.

100%

You have scored 100%.

Congratulations, you have passed the exam.

Reset

Review Assessment

